PRESIDENZA DEL CONSIGLIO DEI MINISTRI

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

# CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

CUP: J51B21005710007
CIG: 9066973ECE

# CONVENZIONE

ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l'affidamento in concessione dei servizi infrastrutturali e applicativi in *cloud* per la gestione di dati sensibili - "Polo Strategico Nazionale"

**Sommario**

**SEZIONE I - DISPOSIZIONI GENERALI** **7**
Articolo 1 PREMESSE E DOCUMENTI CONTRATTUALI 7
Articolo 2 DEFINIZIONI 7
Articolo 3 NORME APPLICABILI 13
Articolo 4 CONDIZIONI GENERALI 13
Articolo 5 OGGETTO 14
Articolo 6 DURATA DELLA CONCESSIONE 16
Articolo 7 SOCIETÀ DI PROGETTO 18
**SEZIONE II – EQUILIBRIO ECONOMICO-FINANZIARIO, RISCHIO E REVISIONE DEL PEF CONTRATTUALE** **19**
Articolo 8 PRESUPPOSTI DELL'EQUILIBRIO ECONOMICO-FINANZIARIO 19
Articolo 9 RISCHI ASSUNTI DAL CONCESSIONARIO 19
Articolo 10 RIPARTIZIONE DEI BENEFICI 20
Articolo 11 REVISIONE DEL PEF 21
Articolo 12 CONTROLLI E COMITATO DI CONTROLLO 24
**SEZIONE III – DELLE OBBLIGAZIONI DEL CONCESSIONARIO E DEL CONCEDENTE** **25**
Articolo 13 SOGGETTI NOMINATI DAL CONCESSIONARIO 25
Articolo 14 OBBLIGAZIONI DEL CONCESSIONARIO 25
Articolo 15 TUTELA DEI LAVORATORI 27
Articolo 16 OBBLIGAZIONI DEL CONCEDENTE 28
Articolo 17 ULTERIORI ATTIVITÀ DEL CONCEDENTE 29
**SEZIONE IV – AVVIAMENTO** **29**
Articolo 18 PIANO FABBISOGNI, PROGETTO DEL PIANO DEI FABBISOGNI, MIGRAZIONE 29
**SEZIONE V - FORZA MAGGIORE E SOSPENSIONE DELLE ATTIVITÀ** **30**
Articolo 19 FORZA MAGGIORE E SOSPENSIONE DELLE ATTIVITÀ 30
**SEZIONE VI - CORRISPETTIVI E PENALI** **31**
Articolo 20 LIVELLI DI SERVIZIO 31
Articolo 21 PENALI 31
Articolo 22 PENALI DEL CONCEDENTE 32
Articolo 23 PENALI DELL'AMMINISTRAZIONE UTENTE 33
Articolo 24 CORRISPETTIVI, PERIODICITÀ DEI PAGAMENTI E FATTURAZIONE 33
Articolo 25 SVINCOLO DELLE GARANZIE 33
**SEZIONE VII - GARANZIE E ASSICURAZIONI** **33**
Articolo 26 GARANZIA DEFINITIVA 34
Articolo 27 POLIZZE ASSICURATIVE 35
Articolo 28 GARANZIE DEL CONCESSIONARIO PER I FINANZIATORI 35

**SEZIONE VIII - VICENDE DELLA CONCESSIONE E MONITORAGGIO** **36**
Articolo 29 SUBAPPALTO E AFFIDAMENTI I DEL CONCESSIONARIO 36
Articolo 30 MODIFICA DELLA CONCESSIONE DURANTE IL PERIODO DI EFFICACIA 36
**SEZIONE IX - CESSAZIONE DEL CONTRATTO** **37**
Articolo 31 EFFICACIA DEL CONTRATTO 37
Articolo 32 CAUSE DI RISOLUZIONE AUTOMATICA 37
Articolo 33 RISOLUZIONE PER INADEMPIMENTO DEL CONCESSIONARIO 37
Articolo 34 SOSTITUZIONE DEL CONCESSIONARIO E SUBENTRO 38
Articolo 35 RISOLUZIONE PER INADEMPIMENTO DEL CONCEDENTE E/O DELL'AMMINISTRAZIONE UTENTE O REVOCA DELLA CONCESSIONE E/O DEL CONTRATTO 39
Articolo 36 EFFICACIA DELLA REVOCA E DELLA RISOLUZIONE E SOMME SPETTANTI AL CONCESSIONARIO 39
Articolo 37 RECESSO 40
Articolo 38 DEVOLUZIONE DELL'INFRASTRUTTURA E CLAUSOLA SOCIALE 41
Articolo 39 VERIFICA DI CONFORMITÀ DELL'INFRASTRUTTURA E DEI SERVIZI 42
**SEZIONE X - ULTERIORI DISPOSIZIONI** **43**
Articolo 40 COMUNICAZIONI 43
Articolo 41 NORME ANTICORRUZIONE E PROTOCOLLI DI LEGALITÀ 43
Articolo 42 OBBLIGHI IN TEMA DI TRACCIABILITÀ DEI FLUSSI FINANZIARI 44
Articolo 43 CONTROVERSIE E FORO COMPETENTE 44
Articolo 44 TRATTAMENTO DEI DATI PERSONALI 44
Articolo 45 REGISTRAZIONE 44
Articolo 46 RINVIO AL CODICE, AL CODICE CIVILE E AD ALTRE DISPOSIZIONI DI LEGGE VIGENTI 44

# CONVENZIONE

L'anno 2022, il giorno 24 del mese di agosto,

tra

il **DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE** della Presidenza del Consiglio dei Ministri con sede in Roma, largo Pietro di Brazzà n. 86, codice fiscale 80188230587, nella persona del Capo Dipartimento *pro tempore* ing. Mauro Minenna, nominato con decreto del Presidente del Consiglio dei ministri 29 marzo 2021, che agisce in qualità di legale rappresentante del Dipartimento *pro tempore*, nato a Bari (BA), il 15 novembre 1969, C.F. MNNMRA69S15A662R ("**Dipartimento**", "**DTD**" o "**Concedente**")

**e**

**La Società Polo Strategico Nazionale S.p.A** ("**PSN S.p.A**.") con sede legale in via Goito 4, numero di iscrizione nel Registro delle Imprese di Roma 1678264, C.F. e Partita IVA 16825251008, in persona del dott. Massimo Mancini, nato a Campobasso (CB) il 12 luglio 1963, C.F. MNCMSM63L12B519G e domiciliato ai fini del presente contratto in via Goito 4, nella qualità di Presidente del Consiglio di Amministrazione e Rappresentante legale.
La Società di Progetto come sopra indicata è costituita dai seguenti operatori economici, già facenti parte del RTI costituito mediante atto per notaio Nicola Atlante in Roma, registrato a Roma il 10 marzo 2022 al n. 2986 serie 1/T, ai fini della partecipazione alla procedura di Gara, tra:

- TIM S.p.A. con sede legale in via G. Negri 1 – 20123 Milano iscritta nel Registro della Imprese di Milano al numero 1580695, C.F. e Partita IVA 00488410010;
- Leonardo S.p.A., con sede legale in Roma, piazza Monte Grappa n. 4, C.F. e iscrizione presso il Registro delle Imprese di Roma 00401990585 e Partita Iva 00881841001;
- SOGEI – Società Generale di Informatica – S.p.A. con sede legale in Roma, via Mario Carucci, n. 99, C.F. e iscrizione nel Registro delle Imprese n. 0327910580, Partita IVA n. 01043931003;
- CDP Equity S.p.A. con sede legale in Milano, via San Marco n. 21/A, C.F. e Partita IVA e iscrizione nel Registro delle Imprese di Milano 07532930968; di seguito per brevità il "**RTI**" o il "**RTI TIM**";

la citata Società di Progetto di seguito, per brevità, denominata "**Concessionario**" è stata costituita, in data 4 agosto 2022, dai membri del predetto RTI secondo le percentuali di partecipazione dallo stesso dichiarate in sede di Gara.

## PREMESSO CHE

1. Le società CDP Equity S.p.A., TIM S.p.A., SOGEI S.p.A. e Leonardo S.p.A. ("**Proponente**") hanno presentato, in forma di costituendo raggruppamento temporaneo di imprese con T.I.M. S.p.A. in qualità di mandataria, ai sensi degli artt. 164, 165, 179, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni ("**Codice**"), una proposta avente ad oggetto l'affidamento di una concessione relativa, in particolare, alla prestazione da parte del Concessionario in favore delle singole Amministrazioni Utenti, in maniera continuativa

e sistematica, di un Catalogo di Servizi, altamente dedicati e con *focus* su sicurezza, connettività ed affidabilità, con messa a disposizione di un'infrastruttura digitale per i servizi infrastrutturali e applicativi in *cloud* per la gestione di dati sensibili - "Polo Strategico Nazionale", appositamente progettata, predisposta ed allestita, ad alta affidabilità, localizzata sul territorio nazionale, con caratteristiche adeguate (con riferimento, in particolare, alla circolare dell'Agenzia per l'Italia Digitale – AgID n. 5 del 30 novembre 2017) ad ospitare la migrazione dei dati frutto della razionalizzazione e consolidamento dei Centri di elaborazione Dati e relativi sistemi informatici delle pubbliche amministrazioni di cui all'articolo 33-*septies* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'articolo 35 del d.l. 16 luglio 2020, n. 76 nonché come ulteriormente modificato dall'art. 7 del d.l. 6 novembre 2021, n. 152 ed a ricevere la migrazione dei detti dati affinché essi siano poi gestiti attraverso una serie di servizi da rendere alle amministrazioni titolari dei dati stessi, vale a dire Servizi Infrastrutturali; Servizi di Gestione della Sicurezza IT; Servizi di *Disaster recovery* e *Business Continuity*; Servizi di Assistenza ai fruitori dei servizi prestati ("**Proposta**").

2. La Proposta era corredata dai documenti richiesti dall'art. 183, comma 15, del Codice, e segnatamente:

   a) progetto di fattibilità tecnico-economica, comprensivo della specificazione delle caratteristiche della gestione, nella forma di un capitolato gestionale;

   b) schema di convenzione, con annessa matrice dei rischi;

   c) piano economico-finanziario, asseverato, con evidenza delle spese sostenute per la predisposizione della Proposta;

   d) dichiarazioni relative al possesso dei requisiti, di cui al comma 17 dell'art. 183 del Codice;

   e) garanzia, ai sensi dell'art. 93 del Codice, e impegno a presentare, in caso di indizione della gara, la garanzia di cui all'art. 183, comma 15, quinto periodo del Codice, calcolata ai sensi dell'art. 183, comma 9, terzo periodo, del Codice, nonché, in caso di aggiudicazione, la garanzia definitiva, di cui all'art. 103 del Codice.

3. La Proposta è stata elaborata con il proposito di inserirsi nell'ambito degli obiettivi indicati dal Piano Nazionale di Ripresa e Resilienza con particolare riferimento agli "Obiettivi Italia Digitale 2026", di cui al d.l. 16 luglio 2020, n. 76, per come convertito dalla legge 11 settembre 2020, n. 120, nonché di quelli dettati dall'Agenzia per l'Italia Digitale - AgID per la realizzazione dell'Agenda Digitale Italiana, in coerenza con gli indirizzi del Presidente del Consiglio dei Ministri e del Ministro delegato.

4. Nello specifico il Piano Nazionale di Ripresa e Resilienza ha previsto specifici obiettivi per la transizione digitale con particolare riferimento agli "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture Digitali" orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni. In questo contesto, e relativamente alla razionalizzazione e al consolidamento dei Data Center della Pubblica Amministrazione, si inserisce l'identificazione e la creazione del "Polo Strategico Nazionale" (nel seguito anche solo "**PSN**"). Conseguentemente, la Proposta è stata espressamente inquadrata dal Proponente nell'ambito del perseguimento degli

obiettivi del Piano Nazionale di Ripresa e Resilienza e, in particolare, in relazione all'obiettivo di «*Digitalizzare la Pubblica Amministrazione italiana con interventi tecnologici ad ampio spettro accompagnati da riforme strutturali*» di cui alla Missione 1, Componente M1C1 che prevede la realizzazione e la messa in esercizio del PSN entro il 31 dicembre 2022.

5. Il DTD ha valutato la Proposta presentata dalla TIM S.p.A., in qualità di mandataria del costituendo RTI con CDP Equity S.p.A., Leonardo S.p.A., Sogei S.p.A., formulando alcune osservazioni, e - al fine di fornire la massima efficacia alla tutela dell'interesse pubblico perseguito - ha invitato il Proponente, ai sensi di quanto previsto dall'articolo 183, comma 15, del Codice dei contratti pubblici, ad apportare specifiche modifiche al progetto di fattibilità, con richiesta a mezzo PEC del 2 dicembre 2021 (protocollo DTD-3651-P e DTD-3652-P); essendosi il Proponente uniformato alle osservazioni ricevute nel termine indicato, la Proposta è stata ulteriormente valutata.

6. Ad esito delle suddette valutazioni, il DTD si è espresso favorevolmente circa la fattibilità della Proposta, in quanto rispondente alla necessità dello stesso di avvalersi di soggetti privati per soddisfare le esigenze delle Amministrazioni per il conseguimento degli obiettivi di pubblico interesse individuati dal Piano Nazionale di Ripresa e Resilienza, dal decreto-legge 16 luglio 2020, n. 76 e dall'Agenzia per l'Italia Digitale per la realizzazione dell'Agenda Digitale Italiana.

7. Il DTD, con provvedimento adottato dal Capo del Dipartimento per la trasformazione digitale n. 47/2021-PNRR, del 27 dicembre 2021, ha dichiarato la Proposta fattibile, ponendola in approvazione e nominando, contestualmente, il Proponente come promotore ("**Promotore**").

8. L'art. 7 del decreto-legge 6 novembre 2021, n. 152, ha disposto che, all'articolo 11 del decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, dopo il comma 3, fosse inserito il comma 3-*bis* secondo cui la Presidenza del Consiglio dei ministri si avvale della società Difesa Servizi S.p.A., di cui all'articolo 535 del decreto legislativo 15 marzo 2010, n. 66, in qualità di centrale di committenza, per l'espletamento delle procedure di gara relative al PSN, di cui all'articolo 33-*septies*, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

9. La convenzione per l'attuazione operativa, la collaborazione e l'attivazione di Difesa Servizi S.p.A. nella funzione di centrale di committenza ai sensi dell'art. 7 del decreto-legge 6 novembre 2021, n. 152 nell'ambito della creazione del PSN è stata sottoscritta, tra Difesa Servizi S.p.A., il Ministero della Difesa e il Dipartimento per l'Innovazione Tecnologica e la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, in data 25 dicembre 2021.

10. Ai fini della citata convenzione, il ruolo di Stazione Appaltante è stato assunto dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri quale Ente Aderente, mentre Difesa Servizi S.p.A. ha agito in qualità di Centrale di Committenza.

11. La Stazione Appaltante, in data 29 dicembre 2021, ha inviato alla Centrale di Committenza, ai sensi di quanto previsto dall'art. 2, comma 6, della predetta Convenzione, formale "atto di attivazione" costituito dai seguenti documenti:
    - decreto n. 47/2021-PNRR del 27.12.2021, motivato ai sensi della legge n. 241 del 1990 e secondo le previsioni della delibera ANAC n. 329 del 21 aprile 2021, con cui ha:

- dichiarato la fattibilità della Proposta presentata dal Proponente nella versione, sostanzialmente e formalmente completa, modificata a seguito delle richieste di modifica formulate dal Dipartimento per la Trasformazione digitale ai sensi dell'articolo 183, comma 15, del Codice;
- approvato, per i motivi esposti in premessa, il progetto di fattibilità della Proposta;
- nominato TIM S.p.A. in qualità di mandataria del costituendo RTI come Promotore ai sensi dell'art. 183, comma 15, del Codice;
- disposto, con determina a contrarre n. 3 del 28/01/2022, di dare corso alle ulteriori attività di cui all'articolo 183, comma 15, del Codice, propedeutiche alla pubblicazione del bando di Gara. La Centrale di Committenza ha indetto, con determina a contrarre n. 3 del 28 gennaio 2022, ai sensi degli artt. 3, comma 1, lett. eee), 60 e 180 nonché art. 183, commi 15 e 16, del Codice, la gara europea, a procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico – privato della realizzazione e gestione del Polo Strategico Nazionale, CIG: 9066973ECE CUP: J51B21005710007, con bando, inviato per la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea in data 28 gennaio 2022 e pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 15 del 04 febbraio 2022.

12. La Commissione giudicatrice, nominata con provvedimento n. 3 del 14 aprile 2022, con verbali n. 5 del 10 giugno 2022, n. 6 del 14 giugno 2022 e n. 7 del 15 giugno 2022, ha formulato la proposta di aggiudicazione a favore del costituendo RTI tra Aruba S.p.A. e Fastweb S.p.A. in qualità di mandataria ("**RTI Fastweb**"). La graduatoria di gara è stata approvata con determina n. 14 del 22 giugno 2022 della Centrale di Committenza e comunicata agli operatori economici partecipanti alla Gara con comunicazioni n. 2402 e n. 2403 di protocollo del 22 giugno 2022. Il Promotore RTI costituito con TIM S.p.A. mandataria, non risultato aggiudicatario, ha esercitato, nel termine previsto dall'art. 183, comma 15 del Codice, con comunicazione del giorno 07 luglio 2022, protocollo in entrata della Centrale di Committenza n. 2362, il diritto di prelazione di cui all'art. 183, comma 15, del Codice, impegnandosi ad adempiere a tutte le obbligazioni contrattuali alle medesime condizioni offerte dall'operatore economico individuato come aggiudicatario originario della procedura di Gara. Il Promotore, con determina di aggiudicazione della Centrale di Committenza n. 15 del 11 luglio 2022, comunicata agli operatori economici partecipanti alla Gara con comunicazioni n. 2681 e n. 2682 di protocollo del 11 luglio 2022, è stato per l'effetto dichiarato nuovo aggiudicatario della procedura.

13. Successivamente all'esercizio del diritto di prelazione, in data 4 agosto 2022, i componenti del RTI Proponente, ai sensi dell'art. 184 del Codice, hanno costituito la Società di Progetto denominata Polo Strategico Nazionale S.p.A., partecipata come segue:

    1) Telecom Italia S.p.A. 45%;

    2) Leonardo S.p.A. 25%;

    3) CDP Equity S.p.A. 20%;

    4) Sogei S.p.A. 10%.

14. La società Polo Strategico Nazionale S.p.A. è subentrata *ex lege* nell'aggiudicazione e, conseguentemente, la citata PSN S.p.A. stipula il presente contratto e assume la qualifica di Concessionario a titolo originario.

15. In data 5 agosto 2022, con nota prot. DICAGP 003392, il Dipartimento per il Coordinamento Amministrativo della Presidenza del Consiglio dei Ministri ha dichiarato la non applicabilità della c.d. normativa *golden power*, di cui al decreto-legge 15 marzo 2012, n. 21, alla stipula della presente convenzione da parte del Concessionario.

16. La Centrale di Committenza, ha comunicato alla Stazione Appaltante in data 23 agosto 2022 (prot. Prot. DTD-3033-A) l'esito delle verifiche dei requisiti generali di cui all'art. 80 del Codice, nonché delle verifiche dei requisiti speciali di cui al paragrafo 7.2 del disciplinare di Gara.

17. Il Concessionario ha provveduto a costituire, ai sensi dell'art. 103 del Codice, la garanzia definitiva, mediante fidejussione assicurativa rilasciata in data 24.08.2022 dalla società Euler Hermes S.A. (NV), polizza n. 2618257.

18. Il Concessionario ha provveduto a presentare idonea documentazione relativa al finanziamento delle attività oggetto di concessione, impegnandosi a sottoscrivere il relativo Contratto di Finanziamento – o a presentare la documentazione attestante la disponibilità delle risorse necessarie, anche proprie – entro 18 (diciotto) mesi dalla sottoscrizione della presente Convenzione.

19. In particolare, tenuto anche conto che le attività oggetto di contratto corrispondono a specifici obiettivi finanziati e contenuti nel PNRR e, nello specifico, ricorrono altresì specifiche e oggettive ragioni di urgenza legate alla necessità di realizzare l'infrastruttura entro il 31 dicembre 2022 (con attività di durata prevista in 120 giorni dalla stipula del contratto), al fine di rispettare quanto precisamente previsto dal cronoprogramma di cui alla Missione 1, Componente M1C1, del PNRR, il presente contratto è stipulato ai sensi di quanto previsto dagli articoli da 48 a 53 del decreto-legge 31 maggio 2021, n. 77, convertito con modificazioni, dalla legge 29 luglio 2021, n. 108, nonché dagli articoli da 2 a 8 del decreto-legge 16 luglio 2020, n. 76, convertito dalla legge 11 settembre 2020, n. 120 e, con particolare riferimento alle disposizioni in materia di documentazione antimafia, ai sensi del combinato disposto degli articoli 53 del decreto-legge n. 77 del 2021, dell'articolo 3 del decreto-legge n. 76 del 2020 e dell'articolo 92, comma 3, del decreto legislativo 6 settembre 2011, n. 159, con la conseguenza che il presente contratto è stipulato sotto condizione risolutiva, ferme restando le verifiche successive ai fini del comprovato possesso dei requisiti e il Concessionario - ove successivamente alle necessarie verifiche dovesse intervenire un provvedimento interdittivo ai sensi della disciplina antimafia in capo al Concessionario ovvero di un suo socio come sopra individuati - accetta che l'Amministrazione contraente procederà al recesso dal presente vincolo contrattuale. Con determina n. 114 del 24 agosto 2022 la Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale in qualità di Stazione Appaltante ha disposto la stipula della presente Convenzione;

20. Le Parti, come sopra individuate, intendono disciplinare, mediante apposita convenzione ("**Convenzione**"), la Concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("**PSN**"), di cui al comma 1 dell'articolo 33-*septies* del d.l. n. 179 del 2012, avente i contenuti

meglio specificati nel seguito.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue:

## SEZIONE I - DISPOSIZIONI GENERALI

### Articolo 1
### PREMESSE E DOCUMENTI CONTRATTUALI

1. Le premesse costituiscono parte integrante e sostanziale della Convenzione.

2. Costituiscono, altresì, parte integrante e sostanziale della presente Convenzione i seguenti allegati:

   i. Allegato A "Capitolato Tecnico e relativi annessi – Capitolato Servizi";
   ii. Allegato B "Offerta Tecnica" e relativi annessi;
   iii. Allegato C "Offerta economica del Fornitore – Catalogo dei Servizi" e relativi annessi;
   iv. Allegato D "Schema di Contratto di Utenza";
   *v.* Allegato E "Facsimile nomina Responsabile trattamento dei dati personali";
   vi. Allegato F "Piano Economico Finanziario asseverato e comprensivo della Relazione Illustrativa" e relativi annessi;
   vii. Allegato G "Matrice dei rischi";
   viii. Allegato H "Indicatori di Qualità";
   ix. Allegato I "Flussi informativi";
   x. Allegato K "DUVRI Contrattuale";
   xi. Allegato L "Elenco dei Servizi Core, no Core e CSP"

### Articolo 2
### DEFINIZIONI

1. Salvo che sia diversamente disposto nella Convenzione, i termini di seguito elencati hanno il seguente significato e si intendono declinati sia al singolare, sia al plurale:

   a. **Amministrazioni**: indica le amministrazioni centrali e locali che sono tenute a raggiungere gli obiettivi di consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese di cui all'art. 33 *septies* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'art. 35, comma 1 del d.l. n. 76/2020 e dall'art. 7, comma 3, lett. c) del decreto-legge 6 novembre 2021, n. 152;

   b. **Amministrazione Utente**: indica l'Amministrazione che effettuano la Migrazione al PSN e stipulano, a condizioni di mercato dietro il pagamento di un prezzo previsto dal Listino Prezzi, il Contratto mediante il Progetto del Piano dei Fabbisogni;

c. **Autorizzazioni**: indica i pareri, le autorizzazioni e tutti gli altri atti di assenso, comunque denominati, necessari per la realizzazione del Servizio;

d. **Bando**: indica il bando che il Concedente ha pubblicato, ai sensi del Codice, per l'affidamento della Concessione;

e. **Beneficio di Rifinanziamento**: ha il significato di cui all'art. 10;

f. **Capitolato Servizi**: indica il documento, inclusivo dei relativi allegati, posto a base di Gara, come eventualmente modificato in sede di Offerta, che indica i termini e condizioni della prestazione delle attività illustrate nel Catalogo dei Servizi;

g. **Caso Base del PEF:** ha il significato del raggiungimento dei Ricavi Core previsti dal PEF;

h. **Catalogo dei Servizi**: indica il documento, inclusivo dei relativi allegati, posto a base di Gara, come eventualmente modificato in sede di Offerta, che elenca i servizi e regolamenta i corrispettivi economici di ogni singolo servizio;

i. **Capitolato Tecnico**: ha il significato di cui all'allegato A;

j. **Centro Servizi**: indica l'insieme di tutte le infrastrutture fisiche (Data Center), delle componenti hardware e software in essi ospitati e delle risorse destinate alla fornitura dei Servizi oggetto del Capitolato Servizi;

k. **Cod. Civ.**: indica il Codice Civile;

l. **Codice**: indica il d.lgs. n. 50/2016 e successive modificazioni o integrazioni, rubricato "Codice dei contratti pubblici";

m. **Codice antimafia**: indica il d.lgs. n. 159/2011 e successive modificazioni o integrazioni, recante il "Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136";

n. **Concedente**: indica il DTD;

o. **Concessionario**: indica la società di progetto denominata Polo Strategico Nazionale S.p.A. che acquisisce ai sensi di legge, a titolo originario, la qualifica di Concessionario;

p. **Concessione**: indica l'insieme dei reciproci diritti e obblighi costituenti il rapporto contrattuale tra Concedente e Concessionario, come regolati dalla Convenzione;

q. **Contratto**: indica il Contratto di Utenza, di cui all'Allegato D, stipulato dall'Amministrazione Utente con il Concessionario, in attuazione della presente Convenzione;

r. **Contratto di Finanziamento**: indica il contratto di finanziamento, o altro accordo vincolante che sarà sottoscritto dal Concessionario con i Finanziatori al fine del reperimento della provvista finanziaria relativa, *inter alia*, a coprire parte dei costi di progettazione, realizzazione e gestione dell'infrastruttura e dei Data Center;

s. **Convenzione**: indica il presente contratto, concluso in modalità elettronica secondo le norme applicabili e mediante scrittura privata, al fine di disciplinare le obbligazioni delle Parti in relazione alla Concessione;

t. **Corrispettivo per il Servizio**: indica le somme dovute dalle Amministrazioni Utenti al Concessionario per la fornitura del Servizio;

u. **Data Center**: indica una struttura fisica, normalmente un edificio compartimentato, unitamente a tutti gli impianti elettrici, di condizionamento, di attestazioni di rete, di cablaggi, ecc. e a sistemi di sicurezza fisica e logica, che in tale edificio sono presenti progettati e allestiti per ospitare e gestire un numero elevato di apparecchiature e infrastrutture informatiche e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale;

v. **Data di Decorrenza del Periodo di Verifica dell'Andamento Commerciale**: indica la data nella quale verrà fatta la verifica del PEF ai sensi dell'art. 11 comma 5;

w. **Direttore dell'Esecuzione o DEC**: indica il direttore dell'esecuzione preposto al controllo sulla regolare esecuzione della Concessione in fase di gestione, e alla verifica che le attività e le prestazioni contrattuali siano eseguite dal Concessionario in conformità della Convenzione, della Documentazione di gara, del Capitolato Servizi e delle norme applicabili;

x. **Direttore del Servizio**: indica il soggetto, nominato dal Concessionario, ai sensi dell'art. 13 della presente Convenzione, incaricato di coordinare la prestazione del Servizio e di tenere i rapporti con il DEC designato dal Concedente e/o dall'Amministrazione Utente;

y. **D.Lgs. 81/08**: indica il d.lgs. n. 81/2008 e successive modificazioni o integrazioni, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;

z. **Documentazione di Gara**: indica, complessivamente, i documenti e gli allegati posti a base di Gara dal DTD per l'affidamento della Concessione;

aa. **DURC**: indica il documento unico di regolarità contributiva;

bb. **DUVRI Contrattuale**: indica il Documento Unico di Valutazione dei Rischi, ai sensi dell'art. 28 del d. lgs. 81/08, concordato all'avvio dell'esecuzione contrattuale tra Concedente e Concessionario;

cc. **Equilibrio Economico-Finanziario**: indica l'equilibrio economico-finanziario degli investimenti e dei costi di gestione della Concessione, identificato in relazione agli Indicatori di Equilibrio. I concetti di «*equilibrio economico e finanziario*», «*convenienza economica*» e «*sostenibilità finanziaria*» sono da intendersi definiti dall'art. 3, comma 1, lett. *fff*) del Codice, che si avrà per qui richiamato;

dd. **Fatto del Concedente e/o dell'Amministrazione Utente**: indica ogni evento imputabile al Concedente e/o all'Amministrazione Utente.

Nello specifico, esso può manifestarsi in occasione di:

i. inadempimento del Concedente e/o dell'Amministrazione Utente alle proprie obbligazioni ai sensi della Convenzione e/o del Contratto;

ii. fatto imputabile al Concedente e/o all'Amministrazione Utente che impedisca al Concessionario di adempiere le proprie obbligazioni, ai sensi della Convenzione e/o del Contratto, ove il Concessionario dimostri di aver diligentemente adempiuto ai relativi oneri, formalità o obbligazioni ai sensi di legge o della Convenzione o del Contratto;

ee. **Finanziatori**: indica gli istituti di credito e/o gli enti finanziatori che hanno sottoscritto ovvero sottoscriveranno il Contratto di Finanziamento e/o gli altri finanziatori terzi della Società di Progetto, inclusi i titolari di titoli e/o obbligazioni emessi ai sensi e in conformità

ai requisiti di cui all'art. 185 del Codice, nonché i loro successori e/o aventi causa a qualsiasi titolo;

ff. **Forza Maggiore**: indica ogni evento, o circostanza, imprevista o imprevedibile al momento della sottoscrizione della Convenzione, al di fuori del ragionevole controllo del Concessionario e del Concedente e ad essi non imputabile, da cui derivi per il Concessionario l'impossibilità, anche temporanea, in tutto o in parte, di adempiere alle proprie obbligazioni, ai sensi della Convenzione, o, comunque, la mancata prestazione dei servizi, per effetto di:

i. guerra, terrorismo, sommossa o simili eventi o circostanze non controllabili che impediscano l'adempimento delle obbligazioni ai sensi della Convenzione;

ii. sabotaggio, attacchi informatici non prevenibili, vandalismo;

iii. esplosioni, radiazioni e contaminazioni chimiche;

iv. dissesto naturale, quali terremoti, inondazioni, alluvioni, allagamenti o simili eventi;

v. epidemie, contagi e pandemie;

vi. sciopero o agitazione sindacale, con espressa esclusione degli eventi esclusivamente relativi ai dipendenti del Concessionario;

vii. impossibilità di accedere a materie prime, apparati o componenti di apparati elettronici o informatici ovvero a servizi necessari;

viii. mancato o ritardato rilascio delle Autorizzazioni da parte delle autorità competenti per cause non imputabili al Concedente e/o all'Amministrazione Utente, né al Concessionario;

ix. provvedimento dell'autorità giudiziaria o di altra autorità pubblica italiana o dell'Unione Europea che determini l'impossibilità, anche solo temporanea, di esercitare la Concessione o porzioni essenziali delle attività o dei presupposti indispensabili di dette attività.

gg. **Gara**: indica la procedura di gara di cui al Bando;

hh. **GDPR**: indica il Regolamento UE 2016/679 in materia di protezione dei dati personali;

ii. **Giorni**: Salvo ove diversamente indicato nella Convenzione, il riferimento ai giorni si intende effettuato a giorni naturali e consecutivi, da computarsi escludendo il primo e comprendendo l'ultimo, a meno che quest'ultimo non cada in un giorno non lavorativo, nel qual caso la scadenza è posticipata al giorno lavorativo immediatamente successivo;

jj. **Indicatori di Equilibrio**: identifica l'indicatore della sostenibilità finanziaria, ossia Debt Service Cover Ratio ("**DSCR**"), e gli indicatori di redditività, ossia il Tasso Interno di Rendimento dell'Azionista ("**TIR dell'Azionista**") e/o del Progetto ("**TIR di Progetto**"), rappresentativi dell'Equilibrio Economico-Finanziario della Concessione, come definiti ed evidenziati nel PEF;

kk. **Infrastruttura**: l'insieme degli asset informatici necessari per la realizzazione e la gestione dell'infrastruttura di cui al comma 1 dell'articolo 33-*septies* del decreto-legge n. 179 del 2012, come esposto negli Allegati A, B e F.

ll. **KPI**: (Key Performance Indicators) ha il significato di cui all'art. 12, comma 3 ed in particolare identifica gli obiettivi che ciascun Contratto tra il Concessionario e le

Amministrazioni Utenti individua e che saranno specificamente individuati nel Contratto con la singola Amministrazione Utente;

mm. **LS o SLA**: indica i livelli qualitativi standard minimi, previsti nel Capitolato Servizi, che devono essere garantiti da parte del Concessionario, nel corso della Concessione, affinché sia assicurata l'adeguatezza del Servizio, come specificati nel Capitolato Servizi;

nn. **Manutenzione Full Risk**: indica la manutenzione delle apparecchiature gestite e comprende tutte le procedure di manutenzione preventiva e di manutenzione correttiva, incluse le parti di ricambio, laddove non specificamente escluse, le spese di viaggio, di trasferta, di manodopera e gli oneri accessori;

oo. **Matrice dei rischi**: indica la tabella descrittiva che identifica i rischi della Concessione e ne descrive l'allocazione a ciascuna delle Parti, allegata alla Convenzione, Allegato G;

pp. **MITD**: indica il Ministro per l'innovazione tecnologica e la transizione digitale;

qq. **Migrazione**: indica il trasferimento dai centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici verso il PSN o verso soluzioni *cloud*;

rr. **Normativa Privacy**: indica il d. lgs. 30 giugno 2003, n. 196 e successive modificazioni o integrazioni, in particolare come adeguato al GDPR, ai sensi del d. lgs. 10 agosto 2018, n. 101;

ss. **Offerta**: indica l'offerta presentata in sede di Gara dall'aggiudicatario;

tt. **Parti**: indica Concedente e Concessionario, congiuntamente intesi.

uu. **PEC:** indica la posta elettronica certificata;

vv. **PEF o Piano Economico Finanziario:** indica l'elaborato elettronico, contenente l'esplicitazione dettagliata dei presupposti e delle condizioni di base che determinano l'Equilibrio Economico Finanziario degli investimenti e della connessa gestione per l'arco temporale di durata della Concessione, asseverato ai sensi di legge, Allegato F comprendente la relativa relazione illustrativa, nonché i successivi aggiornamenti e/o revisioni a seguito di modifiche alla Convenzione o rinegoziazioni del PEF medesimo;

ww. **PEF revisionato**: indica il Piano Economico Finanziario, in formato editabile, che riproduce la proposta di revisione, inclusiva delle misure volte a ripristinare l'Equilibrio Economico e Finanziario;

xx. **Penale**: indica le penali, di cui all'art. 21 della presente Convenzione;

yy. **Periodo di Osservazione**: ha il significato di cui all'art. 10;

**zz.** **Piano dei Fabbisogni:** indica il documento formale predisposto dall'Amministrazione Utente, con l'ausilio del Concessionario, contenente per ciascuna categoria di servizi, indicazioni di tipo quantitativo di ciascun servizio che la stessa intende acquistare in cambio del pagamento di un prezzo;

aaa. **Piano di Migrazione di Massima**: indica l'allegato del Progetto del Piano dei Fabbisogni che contiene l'ipotesi di migrazione del Data Center dell'Amministrazione Utente nel Polo Strategico Nazionale;

bbb. **Piano di Migrazione di Dettaglio**: indica il documento predisposto dal Concessionario a seguito della stipula del Contratto contenente le attività e il piano temporale necessarie alla migrazione del Data Center dell'Amministrazione Utente nel PSN;

ccc. **Piano operativo dell'infrastruttura**: indica il documento progettuale dell'infrastruttura digitale di cui all'art. 5, comma 1 della presente Convenzione redatto e presentato dal Concessionario secondo quanto stabilito dal Capitolato Tecnico e soggetto all'approvazione del Concedente;

ddd. **Prezzo Offerto**: indica il prezzo convenzionato risultante dalla Gara, applicabile al Servizio, a carico delle Amministrazioni Utenti;

eee. **Progetto del Piano dei Fabbisogni**: indica il documento predisposto dal Concessionario e intitolato "Progetto dei Fabbisogni", nel quale sono raccolte e dettagliate le richieste di ciascuna Amministrazione Utente, contenute nel Piano dei Fabbisogni, e la relativa proposta tecnico/economica secondo le modalità tecniche ed i listini previsti rispettivamente nel Capitolato Servizi e nel Catalogo Servizi, che viene allegato al Contratto;

fff. **Progettazione dell'infrastruttura**: indica l'attività di elaborazione dell'infrastruttura digitale di cui all'art. 5 comma 1 della presente Convenzione nonché la successiva redazione del Piano operativo dell'infrastruttura;

ggg. **Proponente**: ha il significato di cui alla premessa 1.;

hhh. **Proposta**: ha il significato di cui alla premessa 1.;

iii. **PSN**: indica il Polo Strategico Nazionale, ovvero l'infrastruttura - di cui al comma 1 dell'articolo 33-*septies* del decreto-legge n. 179 del 2012 - gestita e operata dal Concessionario;

jjj. **Ricavi Core**: indica i ricavi generati dai Servizi Core;

kkk. **Referente del Servizio**: indica il soggetto nominato dal Concessionario, ai sensi dell'art. 12 della presente Convenzione, che avrà il compito di gestire i rapporti con il DEC del DTD e/o dell'Amministrazione Utente per gli aspetti operativi e di coordinamento riguardanti le tematiche di salute e sicurezza sul lavoro;

lll. **Revisione**: indica le procedure, i parametri e le modalità per il ripristino dell'Equilibrio Economico-Finanziario, ai sensi dell'art. 11 della presente Convenzione,

mmm. **Rifinanziamento:** ha il significato di cui all'art. 10;

nnn. **RTI Fastweb**: indica il raggruppamento temporaneo di imprese costituendo fra Fastweb S.pA. mandataria designata e Aruba S.p.A. mandante

ooo. **RTI** o **RTI TIM**: indica il raggruppamento temporaneo di imprese costituito tra TIM S.p.A. mandataria e Leonardo S.p.A., CDP Equity S.p.A. e Sogei S.p.A. mandanti

ppp. **RUP**: indica il responsabile unico del procedimento, nominato dal Concedente e/o dall'Amministrazione Utente, cui è demandata la titolarità del procedimento e della corretta esecuzione della presente Convenzione e/o del Contratto, ai sensi e per gli effetti delle disposizioni di cui agli artt. 31 e 101 del Codice;

qqq. **Servizio**: indica i servizi oggetto di Offerta per la realizzazione del PSN, illustrati nel Catalogo dei Servizi ed i cui termini e condizioni di fornitura sono individuate nel Capitolato Servizi;

rrr. **Servizi Core, no Core e CSP:** hanno il significato di cui all'Allegato L;

sss. **Servizi professionali**: indicano la gestione applicativa, il supporto specialistico, il servizio di assistenza da remoto se richiesto;

ttt. **Sistema Informativo**: indica le dotazioni software e hardware e le relative funzionalità necessarie all'espletamento del Servizio secondo quanto previsto dal Capitolato Servizi;

uuu. **Società di Progetto o SPV**: indica la società che, ai sensi quanto previsto dal disciplinare e da tutti gli atti di gara è stata costituita dal Raggruppamento aggiudicatario e partecipata dai soggetti che, riuniti in raggruppamento temporaneo hanno presentato la Proposta, costituita ai sensi dell'art. 184 del Codice. La predetta Società è stata costituita all'esito di tutti gli adempimenti tecnico-amministrativi connessi con la sua costituzione anche in ordine alla procedura prevista dal rispetto della normativa in materia di Golden Power. La predetta società PSN è subentrata nell'aggiudicazione della procedura al RTI costituito, acquisendo, a titolo originario, la posizione di Concessionario;

vvv. **Soglia Rilevante di Incremento del Rendimento**: ha il significato di cui all'art. 10 della presente Convenzione;

www. **Variazione dell'Equilibrio o Variazione**: indica la variazione dei presupposti, e/o delle condizioni di base dell'Equilibrio Economico Finanziario della Concessione, che sia conseguenza di uno degli eventi indicati al successivo art. 11 e che dia luogo a una modifica degli Indicatori di Equilibrio;

xxx. **Verifica di Conformità**: indica la verifica svolta dal Concedente e/o dall'Amministrazione utente, al termine – rispettivamente - della Concessione e/o del singolo Contratto, ai sensi dell'art. 102 del Codice, finalizzata all'emissione del relativo certificato, che attesta che l'oggetto della Concessione e/o del Contratto, in termini di prestazioni, obiettivi e caratteristiche tecniche, economiche e qualitative, sia stato realizzato ed eseguito nel rispetto delle previsioni contrattuali;

yyy. **Verifica di Conformità dell' infrastruttura:** indica la verifica svolta dal Concedente ai fini e secondo i tempi e le modalità di cui all'art. 6.

## Articolo 3
## NORME APPLICABILI

1. La Concessione è regolata dalla legge italiana e dalla normativa europea applicabile. In particolare, ad essa si applicano le disposizioni espressamente richiamate nella Convenzione e nella Documentazione di Gara, oltre che il Codice.

2. In caso di contrasto, o non perfetta concordanza, tra le disposizioni della presente Convenzione e dei suoi allegati, prevalgono le disposizioni della Convenzione.

## Articolo 4
## CONDIZIONI GENERALI

1. La Convenzione costituisce per le Parti fonte di obbligazioni vincolanti, legittime, valide, azionabili ed eseguibili, in conformità ai rispettivi termini e condizioni. Ferma restando l'ipotesi di sostituzione del Concessionario al ricorrere delle circostanze di cui all'art. 175, comma 1, lett. *d*) del Codice, a pena di nullità la Convenzione non può essere ceduta.

2. In particolare:

   a. il Concessionario ed i suoi soci sono dotati di ogni potere e autorità necessari al fine di

sottoscrivere la Convenzione e adempiere validamente alle obbligazioni da essa nascenti;

b. il Concessionario ed i suoi soci si trovano nel pieno e libero esercizio dei propri diritti, non essendo in stato di insolvenza, liquidazione volontaria, fallimento, liquidazione coatta amministrativa, concordato preventivo o altre simili procedure concorsuali, non essendo in corso alcun procedimento per la dichiarazione di una di tali situazioni;

c. il Concessionario ed i suoi soci che hanno concorso alla determinazione dei requisiti in sede di Gara indetta con il Bando, sono in possesso dei requisiti dichiarati in sede di Gara, nonché di tutti i titoli, le qualifiche e le autorizzazioni necessarie allo svolgimento della propria attività di impresa.

## Articolo 5
## OGGETTO

1. La Convenzione definisce la disciplina generale relativa alla Concessione relativa alla prestazione in favore delle singole Amministrazioni Utenti, in maniera continuativa e sistematica, di servizi altamente dedicati e con *focus* su sicurezza, connettività ed affidabilità, come indicati nell'"Offerta economica del Fornitore – Catalogo Servizi" (Allegato C) e disciplinati nel "Capitolato Tecnico e relativi annessi – Capitolato Servizi" (Allegato A) e nell' "Offerta Tecnica" (Allegato B), con messa a disposizione di un'infrastruttura appositamente progettata, predisposta ed allestita ad alta affidabilità, localizzata sul territorio nazionale, con caratteristiche adeguate ad ospitare la migrazione delle infrastrutture, delle applicazioni e dei dati frutto della razionalizzazione e del consolidamento dei Centri di elaborazione Dati e dei relativi sistemi informatici delle pubbliche amministrazioni di cui all'articolo 33 *septies* del d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'art. 35 del d.l. 16 luglio 2020, n. 76, nonché come ulteriormente modificato dall'art. 7, d.l. 6 novembre 2021, n. 152, ed a ricevere la migrazione dei detti dati affinché essi siano poi gestiti attraverso una serie di servizi da rendere alle amministrazioni titolari dei dati stessi, vale a dire, a titolo esemplificativo e non esaustivo e fermo il rinvio agli allegati,

   [**1**] i "Servizi Core" quali i servizi di (***A***) housing, (***B***) Hosting, (***C***) IaaS Private, IaaS Shared, e (***D***) gli altri servizi di IaaS e Cloud, congiuntamente ai servizi principali di IaaS (Private e Shared); il Concessionario offrirà alle Amministrazioni Utenti una serie di servizi IaaS e Cloud specifici e/o complementari, e in particolare (i) Platform as a Service (PaaS), (ii) Containers-as-a-Service (CaaS), (iii) Disaster Recovery per IaaS e Cloud, (***E***) Hybrid Cloud on PSN Site, (***F***) Public Cloud PSN Managed, (***G***) Secure Public Cloud, (***H***) PaaS Industry, (***I***) Migrazione

   [**2**] i "servizi no Core", quali (***A***) Business & Culture enablement, (***B***) Servizi professionali, (***C***) Replatform e Rearchitect, (***D***) IT infrastructure - service operations.

   Tali Servizi saranno integrati dalle attività di manutenzione di cui all' art. 20 comma 2 della presente Convenzione.

2. Con la stipula della presente Convenzione, il Concessionario si obbliga a prestare alle singole Amministrazioni Utenti che aderiranno alla migrazione stipulando un apposito Contratto i Servizi definiti nel Capitolato Servizi e nel Catalogo dei Servizi.

   A maggiore chiarimento, resta inteso che la presente Convenzione disciplina i termini e condizioni, impegni, obbligazioni e garanzie che sono assunte dal Concessionario e dal

Concedente tra loro. Al contempo i Contratti con le Amministrazioni Utenti, nel rispetto della presente Convenzione, di cui costituiscono applicazione ed adempimento, disciplinano i termini e condizioni, impegni e garanzie delle obbligazioni reciproche assunti dal Concessionario e dalle Amministrazioni Utenti, la validità delle quali è subordinata a quella della presente Convenzione. Conseguentemente, il venire meno della presente Convenzione per qualsiasi causa determina l'inefficacia dell'insieme dei Contratti con le Amministrazioni Utenti. Viceversa, il venir meno del rapporto con la singola Amministrazione Utente non determina l'inefficacia della presente Convenzione. Le obbligazioni assunte dal Concedente con la sottoscrizione della presente Convenzione si rivolgono anche a favore delle singole Amministrazioni Utenti e potranno essere direttamente fatte valere da queste ultime. Allo stesso modo, poiché la sottoscrizione dei Contratti con le Amministrazioni Utenti costituisce adempimento della presente Convenzione, le garanzie e le penali ivi assicurate alle Amministrazioni Utenti saranno da intendersi quali integrative delle garanzie e delle penali previste dalla presente Convenzione.

3. Le specifiche condizioni di fornitura dei Servizi alle singole Amministrazioni Utenti saranno regolate, in base alle esigenze e richieste di ciascuna Amministrazione Utente, tramite apposito Contratto, contenente il Progetto del Piano dei Fabbisogni e sulla base dell'elenco aggiornato delle dotazioni tecnologiche di ciascuna Amministrazione Utente. Alla stipula del Contratto, previo accordo tra le Parti in ordine alla tipologia e misura dei Servizi proposti, sarà possibile procedere con le attività di Migrazione ai sensi dell'art. 33 *septies*, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'art 35 del d.l. 16 luglio 2020, n. 76, nonché come ulteriormente modificato dall'art. 7, d.l. 6 novembre 2021, n. 152 propedeutiche alla fornitura dei Servizi, come disciplinati nel Capitolato Servizi.

4. Resta inteso che, sentito il parere del Comitato di Controllo di cui all'art. 12 della presente Convenzione, il contenuto dei Servizi potrà essere, in coerenza con l'art. 175 del Codice, rideterminato consensualmente tra le Parti allo scopo di assicurare:

   i. l'aggiornamento rispetto alle tecnologie, di tempo in tempo rese disponibili sul mercato, purché con cadenza temporale non inferiore a 24 (ventiquattro) mesi rispetto all'aggiornamento precedente, fissando i corrispettivi per i Servizi così modificati con la determinazione di nuovi prezzi, che potranno essere inferiori o superiori a quelli contenuti nei Contratti originari, fermo restando l'equilibrio del PEF e i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto;

   ii. l'integrazione dei Servizi con la previsione di nuovi servizi, non originariamente previsti dal Catalogo dei Servizi perché frutto dell'evoluzione tecnologica o gestionale, nonché dell'esperienza maturata nella fornitura dei Servizi, purché con cadenza temporale non inferiore a 24 (ventiquattro) mesi rispetto all'aggiornamento precedente; le Parti procederanno alla determinazione dei nuovi prezzi dei Servizi così integrati o aggiornati, fermi restando l'equilibrio del PEF ed i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto;

   iii. la riduzione del Corrispettivo per i Servizi oggetto dell'Offerta, ai limitati fini dell'adeguamento ai prezzi praticati alle Amministrazioni Utenti secondo il mutare della struttura dei costi del Concessionario, che saranno valutati oggettivamente alla luce delle condizioni di mercato dal Comitato di Controllo di cui all'art. 12, fermi restando sia l'equilibrio del PEF che i limiti previsti dalla legislazione vigente per la variazione delle

prestazioni in costanza di contratto; resta altresì inteso e condiviso tra le Parti che il meccanismo di revisione prezzi è quello riportato nell'Allegato B alla presente relativamente all'ID 18 dei punteggi valutativi.

5. Con la stipula della presente Convenzione, il Concessionario si obbliga irrevocabilmente nei confronti del Concedente, oltre che all'adempimento di tutte le obbligazioni che derivano dalla Convenzione o dai Contratti stipulati con le Amministrazioni Utenti, a porre in essere, nei termini di cui alla presente Convenzione: le prestazioni di Progettazione dell'Infrastruttura; la realizzazione dell'Infrastruttura in conformità con il Piano operativo dell'infrastruttura predisposto dal Concessionario ed approvato dal Concedente; gli interventi, su base quinquennale, di ammodernamento tecnologico della Infrastruttura con eventuale sostituzione di sue parti, fermo quanto previsto dal secondo paragrafo del comma 3 che immediatamente precede.

6. Il Concessionario, in osservanza delle norme applicabili, assume i rischi correlati alla Concessione nei termini della Matrice dei Rischi allegata (Allegato G) e remunera gli investimenti sulla base del PEF di Concessione.

   Laddove il rischio assunto dal Concessionario, di tempo in tempo, nel corso della vita della Convenzione, dovesse subire alterazioni in riduzione tali da collocarlo sotto la soglia prevista dalle norme applicabili, le Parti in buona fede rinegozieranno, entro sei mesi dalla comunicazione dell'evento da parte del Concessionario al Concedente, i termini e le condizioni della presente Convenzione in modo da ripristinare le condizioni di legge ed, in caso di mancato accordo, la Convenzione si intenderà risolta. Il Corrispettivo è adeguato annualmente entro il limite del 75% della variazione annua dell'indice ISTAT dei prezzi al consumo delle famiglie di operai e impiegati senza tabacchi. Resta inteso che in sede di adeguamento dei prezzi secondo il citato indice ISTAT, il Concedente verificherà tramite dichiarazione del Concessionario l'andamento contrattuale in relazione all'equilibrio economico finanziario dello stesso ai fini della eventuale rinegoziazione prevista dal presente comma.

## Articolo 6
## DURATA DELLA CONCESSIONE

1. La durata massima della Concessione è di 13 (tredici) anni complessivi decorrenti dalla data di stipula della presente Convenzione. In particolare:
    - è previsto un periodo non superiore a 120 (centoventi) giorni, proposto nell'offerta risultata aggiudicataria, decorrenti dalla sottoscrizione della Convenzione, che dovrà essere destinato alla Progettazione dell'infrastruttura nonché alla sua predisposizione ed allestimento;
    - un periodo di 32 (trentadue) mesi, durante il quale le Amministrazioni potranno stipulare i Contratti, con una durata massima di 10 (dieci) anni, ed effettuare la Migrazione dei dati, servizi e applicazioni.

2. Più in particolare, la durata della Concessione è suddivisa – pur essendo unitario l'oggetto della Convenzione – in due distinti periodi.

   Il primo periodo di Concessione, di non più di 3 (tre) anni dalla sottoscrizione della presente Convenzione sopra citato, sarà destinato, come anticipato, alla Progettazione dell'infrastruttura, alla sua predisposizione ed allestimento oltre che alla stipula dei contratti di utenza. Resta inteso che,

   a. nel corso del periodo di cui al presente comma, a maggiore beneficio dell'interesse pubblico, la prestazione dei Servizi potrà avere luogo con modalità anticipate per quelle porzioni dell'Infrastruttura che siano in grado di essere messe a disposizione della prestazione dei Servizi, purché a fronte della sottoscrizione di singoli Contratti, con anticipo sulla data di avvio del secondo periodo di esecuzione della Convenzione; nel caso di avvio anticipato dei Servizi di cui alla presente lettera, le modalità di prestazione dei Servizi, le relative garanzie e responsabilità saranno disciplinate dal singolo Contratto;

   b. salvo quanto previsto alla lettera a. che immediatamente precede, i Servizi non saranno resi alle Amministrazioni Utenti senza esito positivo della Verifica di Conformità dell'Infrastruttura, che il Concedente si impegna a porre in essere entro 90 (novanta) giorni dalla comunicazione di completamento dell'Infrastruttura che sarà inviata dal Concessionario; le operazioni di verifica e l'esito della Verifica di Conformità dell'Infrastruttura saranno verbalizzate in contraddittorio in un apposito Verbale di Verifica di Conformità.

   Il secondo periodo di Concessione inizierà al termine del primo periodo di Concessione e durerà fino al termine della Concessione indicato al comma 1.

   Il periodo di fornitura dei Servizi alle Amministrazioni Utenti, oggetto dei singoli Contratti, avrà durata di 10 (dieci) anni a decorrere dal completamento della Migrazione della singola Amministrazione utente e comunque non potrà superare la durata della Concessione.

   La durata della Concessione è stata definita nel presupposto che la sottoscrizione del Contratto di Utenza con ciascuna Amministrazione intervenga entro 3 anni dalla stipula della presente Convenzione, salva proroga di quest'ultimo termine concordata tra Concedente e Concessionario (ulteriore rispetto a quella prevista nel successivo comma 8), dovendo poi perfezionarsi la relativa Migrazione entro 48 (quarantotto) mesi dalla stipula della presente Convenzione.

3. Ove il singolo Contratto venisse a scadere in vigenza della Convenzione, l'Amministrazione Utente e il Concessionario potranno, con specifico accordo, prolungare la durata del Contratto sino alla scadenza della Convenzione.

4. Fermo restando quanto previsto al presente articolo, ai sensi dell'art. 175, comma 1, lett. *a*) del Codice, non è ammessa la proroga della Convenzione e dei Contratti.

   Sussiste, tuttavia, l'obbligo, per il Concessionario, di garantire la fornitura dei Servizi, agli stessi prezzi e condizioni previsti dalla presente Convenzione e/o dai Contratti, su richiesta del Concedente e/o dell'Amministrazione Utente, per il periodo strettamente necessario alla conclusione delle eventuali operazioni di gara volte all'affidamento dei Servizi ad un nuovo concessionario. Si precisa che la prosecuzione nella prestazione dei Servizi è ammessa nei soli limitati ed eccezionali casi in cui, per ragioni obiettivamente non dipendenti né dal Concessionario, né dal Concedente e/o dall'Amministrazione Utente, vi sia l'effettiva necessità di assicurare temporaneamente il servizio nelle more dell'individuazione di un nuovo contraente.

   A beneficio di maggiore chiarezza si specifica che, in ogni caso, il Concessionario sarà tenuto a prestare i Servizi nel periodo di estensione di cui al presente comma anche ove sia venuto meno o venga meno nel medesimo periodo l'Equilibrio Economico Finanziario della Concessione, fermo il diritto del Concessionario a vedere ripristinato l'Equilibrio Economico Finanziario della Concessione anche nell'eventuale periodo di estensione della Convenzione ovvero, laddove essa sia venuta meno per qualunque ragione prevista dalla legge o dalla presente Convenzione, a ricevere il relativo indennizzo.

5. Qualora, invece, il Concessionario non sia in grado di garantire, durante il periodo di eventuale estensione di cui ai commi precedenti, la fornitura dei Servizi tramite l'Infrastruttura esistente e vi sia, quindi, la necessità di nuovi investimenti da parte del Concessionario, quest'ultimo e il Concedente negozieranno in buona fede le modalità tecniche per consentire il ristoro della quota di tali investimenti non ammortizzata nel periodo di proroga, sulla base dei parametri del PEF. Resta in ogni caso inteso che non saranno posti in essere da parte del Concessionario ulteriori interventi di ammodernamento dell'infrastruttura secondo quanto previsto dall'art. 5, comma 4.

6. L'estensione dell'efficacia della Convenzione può essere convenuta dalle Parti solo in funzione della Revisione, ai sensi dell'art. 11 della presente Convenzione, o in caso di sospensioni, ai sensi di quanto previsto dal successivo art. 19 della Convenzione, oppure per consentire al Concedente di procedere a quanto necessario per affidare la Concessione ad altro contraente secondo le procedure dovute secondo le norme applicabili.

7. L'estensione dell'efficacia dei singoli Contratti stipulati ed in corso di efficacia con le Amministrazioni Utenti potrà essere posta in essere nelle stesse ipotesi di cui ai commi che immediatamente precedono ovvero, comunque nel limite dell'efficacia della Concessione, nell'ipotesi di cui ai commi 2, lett. *a*) e 3 che precedono.

8. La durata del periodo di Migrazione e di quello di adesione, o anche di uno solo di essi, sarà automaticamente estesa di ulteriori diciotto (18) mesi laddove rispettivamente Migrazione e/o adesione siano, anche solo una di esse, inferiori al Caso Base del PEF.

## Articolo 7
## SOCIETÀ DI PROGETTO

1. Il Concessionario è costituito quale Società di Progetto nei modi e nelle forme indicate dall'art. 184 del Codice nonché dal disciplinare di Gara. La citata Società di Progetto è partecipata dalle società che, in RTI costituito con TIM S.p.A. mandataria, hanno partecipato alla predetta Gara. La Società di Progetto è sottoposta alla normativa dello Stato italiano in materia di *golden power*.

2. In particolare, la partecipazione al capitale sociale - pari complessivamente a € 3.000.000 (tre milioni) - di ciascuna delle società che hanno partecipato alla gara indetta con il Bando in forma di raggruppamento temporaneo è distribuita nei termini seguenti: TIM S.p.A. pari a 1.350 azioni per una percentuale del 45% del capitale; Leonardo S.p.A. pari a 750 azioni per una percentuale del 25% del capitale; CDP Equity S.p.A. pari a 600 azioni per una percentuale del 20% del capitale; e Sogei S.p.A. pari a 300 azioni per una percentuale del 10% del capitale.

3. Come disposto dallo stesso art. 184 del Codice i Servizi oggetto della Convenzione saranno prestati da parte del Concessionario e si intendono realizzati e prestati in proprio anche nel caso in cui siano affidati dal Concessionario direttamente ai propri soci che siano in possesso dei requisiti stabiliti dalle norme applicabili, ferma la possibilità di ricorrere al subappalto, per come disciplinato dall'art. 174 del Codice e ad altre tipologie contrattuali diverse dal subappalto, inclusi i subcontratti, in conformità con le norme applicabili. A tal fine, il Concessionario garantisce che i soci cui sono affidati direttamente i Servizi, indipendentemente dalla relativa quota di partecipazione nella Società di Progetto, li eseguano nel rispetto delle prescrizioni di Legge e del contenuto dell'Offerta.

4. Fermo restando che, salvo quanto previsto dagli artt. 48, commi 17, 18 e 19 e 175, comma 1, lett. *d*), n. 2 del Codice, i soci che hanno concorso a formare i requisiti per la qualificazione sono tenuti a partecipare alla Società di Progetto e a garantire, nei limiti di legge, il buon adempimento degli obblighi del Concessionario, le partecipazioni dagli stessi detenute nella Società di Progetto potranno essere liberamente cedute tra gli stessi soci.

   Resta altrettanto fermo che i soci che siano investitori istituzionali che non abbiano concorso a formare i requisiti per la qualificazione possono cedere la loro partecipazione in qualsiasi momento ad altri investitori istituzionali ovvero agli altri soci.

   L'ingresso di nuovi soci nel capitale del Concessionario che non siano investitori istituzionali, incluso quello derivante dalla cessione di partecipazioni da parte dei soci qualificanti in aggiunta a quelli che hanno concorso a formare i requisiti per la qualificazione, è subordinato, a pena di risoluzione per inadempimento del Concessionario ai sensi dell'articolo 33 della Convenzione, al consenso del Concedente.

   Di tutte le variazioni nel capitale sociale del Concessionario, quest'ultima si impegna ad informare tempestivamente il Concedente che, ove richiesto, si obbliga a rilasciare il relativo consenso entro 30 (trenta) giorni dal ricevimento della richiesta da parte del Concessionario restando inteso che, a termini dell'art. 20 della l. 7 agosto 1990, n. 241, decorso detto termine senza che sia pervenuto il diniego del consenso del Concedente, la modifica della compagine societaria si intende accettata e diviene pertanto efficace.

5. Il Concessionario assume altresì l'obbligo di comunicare al Concedente, senza indugio, ogni notizia o fatto che possa determinare la perdita dei requisiti per la qualificazione o la loro riduzione al di sotto della misura dimostrata in sede di Gara indetta sulla base del Bando ed a porvi rimedio entro il termine perentorio a tal fine assegnato dal Concedente.

## SEZIONE II – EQUILIBRIO ECONOMICO-FINANZIARIO, RISCHIO E REVISIONE DEL PEF CONTRATTUALE

### Articolo 8
### PRESUPPOSTI DELL'EQUILIBRIO ECONOMICO-FINANZIARIO

1. La disciplina della Concessione si fonda sul rispetto dell'Equilibrio Economico-Finanziario, cristallizzato nel PEF, sulla base dei presupposti e delle condizioni previsti nel medesimo PEF, nonché in ossequio all'allocazione dei rischi, riportata nella Matrice dei rischi, allegata alla Convenzione (Allegato G).

2. Ai sensi dell'art. 165 del Codice, i ricavi di gestione del Concessionario provengono dalla fornitura dei Servizi alle Amministrazioni Utenti, secondo i prezzi previsti dal PEF per ciascun Servizio. Il puntuale ed esatto pagamento da parte del Concedente e delle Amministrazioni Utenti degli importi dovuti ai sensi della presente Convenzione costituisce uno degli elementi principali su cui si fonda l'Equilibrio Economico-Finanziario della Concessione.

### Articolo 9
### RISCHI ASSUNTI DAL CONCESSIONARIO

1. Il Concessionario assume su di sé i seguenti rischi, costituiti, in specifico, da:

   a. rischio di domanda, in relazione:

      (i) al numero di Amministrazioni Utenti che decideranno di migrare e che perfezioneranno il processo di Migrazione;

      (ii) alla quantità e tipologia di Servizi che le Amministrazioni Utenti, che hanno perfezionato la Migrazione richiederanno, mediante la sottoscrizione dei Contratti;

      trovando applicazione quanto previsto al successivo art. 11, comma 5;

   b. rischio di disponibilità, relativo alla costante disponibilità degli impianti e dotazioni tecnologiche infrastrutturali dei Data Center, secondo i requisiti ed i LS stabiliti nel Capitolato Servizi. In particolare, il rischio si concretizza in relazione alla possibilità di aumento dei costi di gestione e manutenzione degli impianti e dotazioni tecnologiche infrastrutturali dei Data Center e delle componenti edili ad essi relativi, compresa la loro eventuale sostituzione, e, in generale, dei costi necessari a garantire i LS del Servizio, sotto il profilo della gestione e del personale utilizzato, (a tal proposito si richiamano le migliorie degli indicatori di qualità riportate nell'Allegato H alla presente Convenzione).

   c. rischio di gestione, legato ad una errata valutazione, da parte del Concessionario, dei prezzi praticati per i Servizi nonché all'incremento dei costi di fornitura dei Servizi medesimi;

   d. rischi di investimento, legati all'approvvigionamento delle componenti degli impianti e dotazioni tecnologiche infrastrutturali dei Data Center, funzionali alla fornitura del Servizio;

   e. rischio di finanziamento della Concessione, ovverosia di mancato reperimento delle risorse di

finanziamento a copertura dei costi e nei tempi prestabiliti ai sensi dell'articolo 180, comma 7, (a tal proposito si richiama quanto contenuto negli Allegati B e G alla presente Convenzione);

f. rischio di progettazione, predisposizione e allestimento, in relazione alle variabili tecnologiche e operative;

il tutto nei termini specificati nella Matrice dei rischi, allegata alla Convenzione (Allegato G).

**Articolo 10**
**RIPARTIZIONE DEI BENEFICI**

1. A partire dalla Data di Decorrenza del Periodo di Verifica dell'Andamento Commerciale della Concessione, qualora per effetto di una adesione al PSN superiore a quella prevista ai sensi del PEF, i ricavi effettivamente percepiti dal Concessionario al netto dei costi effettivamente sostenuti, comprensivi di imposte e detrazioni dovute ad ogni titolo, presenti e future dovessero determinare un incremento del TIR di Progetto in misura superiore del 2% (due per cento) rispetto al livello previsto nel PEF quale indicatore dell'Equilibrio Economico Finanziario (la "**Soglia Rilevante di Incremento del Rendimento del TIR di Progetto**"), il Concessionario rimodulerà per il periodo rimanente i prezzi in modo da retrocedere al Concedente e/o alla Amministrazione Utente la quota parte di beneficio eccedente la Soglia Rilevante di Incremento del Rendimento, fermo restando l'Equilibrio Economico Finanziario come di tempo in tempo aggiornato.

2. A tale fine, a partire dalla Data di Decorrenza del Periodo di Verifica dell'Andamento Commerciale della Concessione e sino al termine della Concessione, il Concessionario ed il Concedente provvederanno ad effettuare aggiornamenti periodici del PEF su base biennale (il "**Periodo di Osservazione**"). Ove occorrer possa, resta inteso che eventuali proventi percepiti da parte del Concessionario in ciascun Periodo di Osservazione e tali da non determinare un'eccedenza rispetto alla Soglia di Rilevanza di Incremento del Rendimento restano di esclusiva pertinenza del Concessionario e non sono (né potranno) essere oggetto dei meccanismi di condivisione di cui al presente articolo.

3. Qualora il Concessionario, nel corso della durata della Concessione, intenda effettuare un'operazione volta:

   a. ad estinguere, totalmente o parzialmente, le fonti di debito contratte con gli istituti finanziatori e riflesse nel PEF e/o rifinanziare tali fonti di debito (in qualsivoglia forma tecnica, ivi incluso, ove del caso, attraverso ricorso al mercato dei capitali mediante l'emissione di obbligazioni e/o titoli di debito); ovvero

   b. a rinegoziare e/o rimodulare le condizioni delle fonti di debito contratto con gli istituti finanziatori e riflesse nel PEF;

   dovrà darne comunicazione scritta al Concedente, fornendogli le necessarie informazioni circa i tempi, i costi e le condizioni del nuovo finanziamento (il "**Rifinanziamento**").

   Qualora per effetto del Rifinanziamento: a) si verifichi un incremento delle obbligazioni e responsabilità del Concedente; e/o b) il quadro delle garanzie esistenti a favore del Concedente risulti diminuito; e/o c) il Concedente risulti soggetto a impegni aggiuntivi, il Rifinanziamento non potrà essere perfezionato senza la previa approvazione del Concedente, che non potrà essere irragionevolmente negata.

Qualora il Rifinanziamento comporti dei benefici per il Concessionario tali da determinare un incremento del TIR dell'Azionista in misura superiore del 1,8% (unovirgolaotto per cento) rispetto al livello previsto nel PEF quale indicatore dell'Equilibrio Economico Finanziario, verificati attraverso l'inserimento delle opportune modifiche nel Piano Economico Finanziario contrattuale (il "**Beneficio da Rifinanziamento**"), detto Beneficio da Rifinanziamento, calcolato dal Concessionario e comunicato al Concedente, sarà condiviso con il Concedente in misura pari a un massimo del 33% (trentatrè per cento).

A miglior chiarimento di quanto precede, si precisa che il TIR dell'Azionista ed il TIR di Progetto potranno conseguentemente variare in aumento (rispetto al valore indicato nel PEF) per effetto delle disponibilità di cassa derivanti dal (o altrimenti connesse al) Beneficio da Rifinanziamento.

4. Resta inteso che nel caso in cui, alla data del Rifinanziamento, la Convenzione versasse in una situazione di alterazione dell'Equilibrio Economico Finanziario, l'eventuale Beneficio da Rifinanziamento sarà integralmente riservato alla (e pertanto trattenuto dal) Concessionario escludendo per tale ipotesi la ripartizione con il Concedente, fermo restando in ogni caso il diritto del Concessionario di attivare la procedura di riequilibrio ai sensi della presente Convenzione e di ottenere il ripristino degli Indicatori di Equilibrio.

   Resta altresì inteso e convenuto tra le Parti che le disponibilità di cassa derivanti dal (o altrimenti connesse al) Beneficio da Rifinanziamento

   a. qualora di spettanza del Concessionario ai sensi del presente articolo saranno considerate come liberamente disponibili da parte del Concessionario e saranno in ogni caso da questo trattenute anche al fine di prevederne la distribuzione in favore dei soci sotto forma di dividendi o in qualsivoglia altra forma;

   b. qualora di spettanza del Concedente ai sensi del presente articolo saranno retrocesse secondo le modalità che saranno di volta in volta determinate in buona fede di comune accordo tra Concedente e Concessionario.

## Articolo 11
## REVISIONE DEL PEF

1. Gli elementi indicati all'art. 8 della presente Convenzione costituiscono i presupposti dell'Equilibrio Economico-Finanziario.

2. Le Parti prendono atto che l'Equilibrio Economico-Finanziario è espresso, in particolare, dai seguenti Indicatori di Equilibrio, valutati congiuntamente, contenuti nel PEF contrattuale:

   a. TIR di Progetto, al netto delle imposte, pari a 5,1% (cinquevirgolauno per cento);

   b. DSCR minimo, almeno pari a 1,4 (unovirgolaquattro).

3. Qualora si riscontri una Variazione dell'Equilibrio, nel rispetto di quanto disposto dalla normativa in materia e ferma restando la permanenza dei rischi allocati in capo al Concessionario, le Parti convengono di procedere alla Revisione del PEF contrattuale e della Convenzione, sempreché la Variazione dell'Equilibrio sia determinata da eventi non imputabili al Concessionario.

4. Rientrano tra tali eventi solo le seguenti fattispecie:

a. eventi di Forza Maggiore;

b. l'inadempimento o il ritardato adempimento da parte del Concedente e/o dell'Amministrazione Utente, ovvero la variazione della durata della Concessione non imputabile al Concessionario o la variazione del rischio di credito delle Amministrazioni Utenti conseguente al ritardato o mancato pagamento dei corrispettivi dei Servizi da parte delle stesse;

c. l'entrata in vigore di norme legislative e regolamentari che incidano sui termini e sulle condizioni di progettazione, predisposizione ed ammodernamento quinquennale dell'Infrastruttura nonché di prestazione dei Servizi, con particolare riferimento ai relativi costi e tempi, tali da determinare una variazione negativa del TIR del progetto superiore allo 0,17% (zerovirgoladiciassette per cento) o la riduzione DSCR minimo ad un livello inferiore a 1.3 X (unovirgolatre) (a tal proposito, si rinvia a quanto riportato nell'Allegato B e la voce "mutamenti imposti ex lege" dell'Allegato G).

5. Le Parti, fatto salvo quanto previsto ai commi 8 e 10, convengono di procedere alla revisione del PEF contrattuale e della Convenzione, oltre che al verificarsi di una Variazione dell'Equilibrio dovuta a una delle fattispecie di cui al comma 4, anche laddove, al trentesimo (30°) mese dalla stipula della presente Convenzione, per effetto di un evento non imputabile al Concessionario la Variazione dell'Equilibrio determini un TIR di progetto, al netto delle imposte, inferiore al 2,2% (duevirgoladue per cento) come previsto nell'allegato G - "matrice dei rischi" voce "rischio di domanda".

6. Al verificarsi di una Variazione dell'Equilibrio, dovuta a una delle fattispecie, di cui ai commi 4 e 5 del presente articolo, al fine di avviare la relativa procedura di Revisione, il Concessionario ne dà comunicazione per iscritto al Concedente, con esatta indicazione dei presupposti che hanno determinato la Variazione dell'Equilibrio, supportata da idonea documentazione dimostrativa, che deve consistere nella presentazione di:

a. PEF, in formato editabile, in disequilibrio;

b. PEF revisionato, in formato editabile, che riproduce la proposta di Revisione;

c. relazione esplicativa al PEF revisionato, che illustri anche i presupposti che hanno condotto alla richiesta di Revisione;

d. relazione dimostrativa dell'evento non imputabile al Concessionario e dei maggiori oneri da esso derivanti;

e. schema di atto aggiuntivo per il recepimento in Convenzione di quanto previsto nel PEF revisionato.

7. La Revisione è finalizzata a determinare il ripristino degli Indicatori di Equilibrio, nei limiti di quanto necessario alla sola neutralizzazione degli effetti derivanti da uno, o più, eventi non imputabili al Concessionario e che hanno dato luogo alla Revisione.

8. Il Concedente, previo gradimento del Concessionario, nell'ipotesi di cui al comma 5, nominerà un soggetto terzo indipendente, in possesso di specifica ed elevata competenza in materia economica e di revisione legale, a cui sarà chiesto di verificare la correttezza dei criteri di esposizione del PEF

in disequilibrio anche in contraddittorio con il Concessionario. Tale verifica dovrà avere ad oggetto in particolare la coerenza di quanto indicato nella documentazione di cui al comma 6 con quanto previsto nel PEF sia in riferimento alla componente fissa necessaria per la realizzazione dell'Infrastruttura di base oggetto della Convenzione, con particolare riguardo agli investimenti correlati agli elementi caratterizzanti la Proposta, sia in riferimento alla componente variabile proporzionale alle previsioni dei volumi in ingresso secondo i profili delle adesioni ricevute in fase di esecuzione del Contratto. Tale procedura dovrà concludersi entro 90 (novanta) giorni dalla comunicazione di cui al comma 6.

9. Al fine di consentire le valutazioni di cui ai commi precedenti le Parti si accorderanno, contestualmente alla sottoscrizione della presente Convenzione, sul livello di dettaglio e sulla frequenza di consuntivazione dei KPI finanziari e operativi necessari a valutare correttamente costi, ricavi e sottoscrizione dei Servizi.

10. Se all'esito della valutazione di cui al comma 8 emerge che la Variazione dell'Equilibrio persiste anche scorporando le componenti di investimento e di costo non coerenti con il PEF, le Parti procedono alla revisione del PEF contrattuale e della Convenzione escludendo gli elementi economici valutati come non coerenti dal soggetto terzo indipendente di cui al comma 8.

11. In tutti i casi di revisione del PEF contrattuale di cui ai precedenti commi 4 e 5, verrà costituito un tavolo tecnico composto da rappresentanti delle Parti che dovrà riunirsi con periodicità settimanale e giungere ad una valutazione conclusiva in ordine alle misure volte a consentire il riequilibrio del PEF. Se le Parti non trovano accordo sulla Revisione entro 180 (centottanta) giorni, le Parti possono recedere dalla Convenzione, in attuazione dell'art. 165, ultimo comma del Codice. In tal caso, si applica l'art. 37 della Convenzione. Il mancato accordo non potrà essere configurato come inadempimento della Concessione.

12. Nel caso di richiesta, da parte del Concedente, di varianti che comportino un aumento degli investimenti, o dei costi del Concessionario, ai sensi di quanto previsto all'art. 175 del Codice e all'art. 30 della Convenzione, si può procedere, indipendentemente dalla percentuale di alterazione degli indicatori della Variazione dell'Equilibrio, di cui alle definizioni dell'art. 2 della Convenzione, mediante Revisione del PEF. Alternativamente, in tali casi, si può procedere mediante il pagamento, da parte del Concedente, degli importi corrispondenti alla variante, senza attivare il meccanismo di Revisione, di cui al presente articolo.

## Articolo 12
## CONTROLLI E COMITATO DI CONTROLLO

1. Il Concessionario si impegna, a seguito della stipula della presente Convenzione, a trasmettere al Concedente le informazioni sull'andamento della presente Convenzione e dei prezzi, tempi e modalità praticati per i Servizi, ai sensi di quanto previsto dall'Allegato I "Flussi informativi".

2. Entro 3 (tre) mesi dall'avvio della prestazione dei Servizi alla prima Amministrazione Utente, il Concedente ed il Concessionario daranno vita ad un Comitato di Controllo composto da un numero di membri che assicuri la eguale rappresentanza del Concedente e del Concessionario e che, di norma, si riunirà con cadenza almeno trimestrale.

3. Il Comitato di Controllo ha potere di vigilanza sull'andamento della Concessione e può suggerire al Concedente, al Concessionario o ad entrambi misure di miglioramento dei Servizi, qualora non risultino in linea con i KPI prefissati, anche su segnalazione di singole Amministrazioni Utenti.

4. Spetta al Comitato di Controllo la verifica dell'andamento dei prezzi dei Servizi e degli altri termini ai quali questi sono resi alle Amministrazioni Utenti, in relazione ai prezzi ed alle tecnologie comparabili presenti sul mercato, avendo sempre riguardo all'incidenza sull'equilibrio del piano economico finanziario.

5. Il Comitato di Controllo ha altresì il compito di supportare il Concedente e il Concessionario attraverso:

   a. l'espressione del parere consultivo di cui al precedente art. 5, comma 4 e l'effettuazione delle valutazioni di cui al punto iii. di tale comma;

   b. l'esame ai sensi del successivo art. 17, comma 2, degli esiti dell'attività di verifica e controllo di cui al comma 1 del medesimo articolo;

   c. l'esame della questione di cui al successivo art. 18, comma 6, formulando valutazioni e/o proposte da sottoporre all'Amministrazione Utente interessata;

   d. l'esperimento del tentativo di conciliazione di cui al successivo art. 22, comma 3;

   e. l'effettuazione della valutazione di cui al successivo art. 38, comma 2, anche avvalendosi, se ritenuto opportuno, della collaborazione di esperti in possesso di specifica ed elevata competenza in materia tecnico informatica.

   Inoltre, il Comitato di Controllo svolge i compiti ad esso assegnati e regolati nello schema di Contratto allegato (Allegato D).

## SEZIONE III – DELLE OBBLIGAZIONI DEL CONCESSIONARIO E DEL CONCEDENTE

### Articolo 13
### SOGGETTI NOMINATI DAL CONCESSIONARIO

1. Il Concessionario, entro 20 (venti) giorni dalla sottoscrizione della Convenzione, nomina e comunica al DTD al seguente indirizzo PEC diptrasformazionedigitale@pec.governo.it un soggetto adeguatamente qualificato come Direttore del Servizio, unico interlocutore del RUP e del DEC del Dipartimento, nonché delle singole Amministrazioni Utenti, per tutta la durata della Concessione.

2. Sempre entro 20 (venti) giorni dalla sottoscrizione della Convenzione, il Concessionario nomina e comunica al DTD un soggetto adeguatamente qualificato come Referente del Servizio, con il compito di gestire i rapporti con il DEC del Dipartimento e/o della singola Amministrazione utente, per gli aspetti operativi e di coordinamento riguardanti le tematiche di salute e sicurezza sul lavoro.

3. In caso di indisponibilità, a qualsiasi causa dovuta, del Direttore o del Referente del Servizio, per più di 4 (quattro) settimane, o di sua sostituzione, il Concessionario deve darne comunicazione al Concedente, con le formalità di cui all'art. 40 della Convenzione.

## Articolo 14
## OBBLIGAZIONI DEL CONCESSIONARIO

1. All'avvio del Servizio, il Concessionario ha l'obbligo di garantire, a proprie spese e nei termini previsti dalla Convenzione, la fornitura dei Servizi, così come meglio dettagliata nell'Offerta e nel Capitolato Servizi.

2. Il Concessionario si obbliga, in particolare:

   2.1. a favore del Concedente, a:

   a. progettare, predisporre, allestire e mettere a disposizione l'Infrastruttura impiantistica e tecnologica, con caratteri di alta affidabilità, nei termini di cui al Capitolato Tecnico;

   b. ottenere ogni autorizzazione eventualmente necessaria per la progettazione dell'Infrastruttura, il suo allestimento e la messa in esercizio e la conduzione dei Servizi;

   c. garantire la disponibilità dei locali ospitanti i Data Center;

   d. sottoscrivere il Contratto di Finanziamento, trasmettendone copia comprensiva di tutti i documenti allegati sottoscritti con i Finanziatori e degli eventuali contratti di copertura del rischio di variazione dei tassi d'interesse con i relativi allegati, entro e non oltre diciotto (18) mesi dalla stipula della presente Convenzione, pena la risoluzione della stessa come previsto dall'art. 32 della presente Convenzione, resta salva la facoltà del concessionario di reperire la liquidità necessaria mediante risorse proprie ovvero attraverso altre forme di finanziamento previste dalla normativa vigente, purché sottoscritte entro lo stesso termine rilasciate da operatori di cui all'art. 106 del D.lgs. n. 385 del 01 settembre 1993;

   e. mantenere attive ed efficaci le garanzie prestate secondo i termini della presente Convenzione;

   f. non cedere a terzi la presente Convenzione;

   g. indicare il Codice Univoco di progetto (CUP) oltre al Codice identificativo di Gara (CIG) nei Contratti e negli atti rivolti al Concedente che integrino o modifichino la presente Convenzione nelle ipotesi dalla Convenzione stessa previste;

   h. adempiere alle altre obbligazioni espressamente previste dalla presente Convenzione.

   2.2. a favore delle Amministrazioni Utenti, a:

   a. prestare i Servizi secondo i termini e le condizioni disciplinati dal Contratto ed in ossequio al Capitolato Servizi e all'Offerta.

3. Resta inteso che le prestazioni del Concessionario potranno essere rese in nome e per conto dello

stesso da parte dei soci che abbiano assunto la qualità di Proponente, ovvero da società dagli stessi controllate, fermo restando che il Concessionario resterà l'esclusivo responsabile dell'esatta esecuzione della Convenzione e dei Contratti con le Amministrazioni, rispondendo verso il Concedente e le Amministrazioni Utenti degli eventuali inadempimenti dei subappaltatori.

4. Il Concessionario si impegna altresì a:

   a) organizzare una banca dati, per come descritta negli Allegati A "Capitolato Tecnico e relativi annessi – Capitolato Servizi" e B "Offerta Tecnica del Fornitore"; contenente dati, documenti, informazioni e notizie di rilievo concernenti l'adempimento delle prestazioni contrattuali, alimentata dal Concessionario stesso ed accessibile al Concedente ed alle Amministrazioni Utenti in tempo reale;

   b) su richiesta del Concedente, fornire tempestivamente al Concedente medesimo, anche su supporto elettronico, la documentazione, le informazioni e le notizie comunque utili alla verifica del rispetto da parte del Concessionario degli obblighi posti dalla presente Convenzione e pubblicare tali documenti sul proprio sito web;

   c) fornire al Responsabile del Procedimento tutti i chiarimenti richiesti;

   d) partecipare alle visite che il Responsabile del Procedimento e/o suoi incaricati effettuano al fine di svolgere i controlli e le verifiche di competenza;

   e) informare tempestivamente il Concedente in relazione a: (*i*) ogni circostanza o evento che potrebbe comportare sia ritardi nell'erogazione dei Servizi, sia indisponibilità, anche parziale, degli stessi; (*ii*) la sussistenza di fatti o circostanze in grado di configurare, anche solo potenzialmente, presupposto per la risoluzione della, recesso o decadenza dalla presente Convenzione; (*iii*) la sussistenza di fatti o circostanze in grado di configurare, anche solo potenzialmente, presupposto per la mancata erogazione o decadenza dal beneficio del termine delle linee di credito rilasciate al Concessionario ai sensi del Contratto di Finanziamento, per il mancato collocamento delle obbligazioni emesse dal Concessionario ovvero per l'esercizio da parte dei Finanziatori di facoltà volte a limitare l'operatività del Concessionario o l'escussione di garanzie e impegni previsti nel Contratto di Finanziamento, a carico del Concessionario o dei soci; (*iv*) le controversie, i procedimenti giurisdizionali, avanti a qualsiasi giurisdizione, da parte o nei confronti del Concessionario e di ciascuno dei soci che possano pregiudicare la loro capacità di adempiere agli obblighi derivanti dal Contratto; (*v*) ogni altro evento, circostanza o provvedimento che possa avere effetto pregiudizievole sulla Convenzione ovvero sulla capacità del Concessionario di adempiervi;

   f) inviare trimestralmente adeguate informazioni economiche, finanziarie e gestionali sulle attività oggetto di Concessione, al fine di consentire l'esercizio del potere di controllo da parte del Concedente, in conformità al paragrafo 7.1 delle Linee Guida ANAC n. 9 recanti «*Monitoraggio delle amministrazioni aggiudicatrici sull'attività dell'operatore economico nei contratti di partenariato pubblico privato*», secondo le specifiche che saranno concordate dalle Parti entro novanta (90) giorni dalla sottoscrizione della presente Convenzione;

5. Il Concessionario si impegna ad adempiere agli obblighi informativi di cui al presente articolo, ove non specificato, entro trenta (30) giorni dal ricevimento della richiesta scritta nonché si impegna al rispetto di tutte le prescrizioni e obblighi ricadenti in capo al Responsabile del trattamento di cui all'allegato E.

6. Il Concessionario si impegna a consegnare al Concedente e/o alle Amministrazioni utenti, entro 6 (sei) mesi dalla conclusione della presente Convenzione, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato delle assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta.

7. Analogamente a quanto previsto per il rapporto sulla situazione del personale di cui all'articolo 47 comma 2, del decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n.108, la relazione di cui al precedente comma deve essere trasmessa alle rappresentanze sindacali aziendali ed al consigliere e alla consigliera regionale di parità. La mancata produzione della relazione di genere sulla situazione del personale maschile e femminile, costituendo obbligo da adempiere a valle della stipulazione della presente Convenzione, conduce all'applicazione della penale di cui al comma 6 dell'articolo 47, pari ad € 1.000,00 (euro mille/00) per ogni giorno di ritardo.

8. Il Concessionario si impegna a consegnare al Concedente, entro sei mesi dalla stipula della Convenzione, una dichiarazione del legale rappresentante che attesti la regolarità rispetto alle norme che disciplinano il diritto al lavoro delle persone con disabilità, nonché una relazione che chiarisca l'avvenuto assolvimento degli obblighi previsti a carico delle imprese dalla legge 12 marzo 1999, n. 68, e illustri eventuali sanzioni e provvedimenti imposti a carico delle imprese nel triennio precedente la data di scadenza della presentazione delle offerte. Tale relazione deve essere trasmessa anche alle rappresentanze sindacali aziendali e, in difetto, si applicherà la penale di cui al comma 6 dell'articolo 47, pari ad € 1.000,00 (euro mille/00) per ogni giorno di ritardo.

9. Il Concessionario si impegna, pena la risoluzione della Convenzione, a realizzare e gestire il Polo Strategico Nazionale nel pieno rispetto del *"Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione"*, adottato dall'AgID – con Determinazione n. 628/2021 del 15 dicembre 2021 - in conformità alle previsioni di cui all'articolo 33-*septies*, comma 4, del d.l. 179/2012 e all'articolo 17, comma 6, del decreto-legge n. 82/2021, e nel rispetto degli atti esecutivi dello stesso Regolamento adottati dall'Agenzia per la cybersicurezza nazionale, d'intesa con il Dipartimento per la trasformazione digitale. A tal proposito si rimodula la Matrice dei rischi inserendo tale rischio normativo con ripartizione del rischio 100% in capo al Concessionario;

10. Il Concessionario dichiara che il RTI ha assolto, al momento della presentazione dell'offerta stessa, gli obblighi in materia di lavoro delle persone con disabilità di cui alla legge 12 marzo 1999, n. 68;

11. Il Concessionario è consapevole e accetta che, in relazione alla presente Convenzione: il Concedente si avvarrà della clausola risolutiva espressa di cui all'art. 1456 c.c. ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale, o dei dirigenti dell'impresa con funzioni specifiche relative all'affidamento alla stipula e all'esecuzione del contratto sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319-*bis*, 319-*ter*, 319-*quater*, 320, 322, 322-*bis*, 346-*bis*, 353 e 353-*bis*, del codice

penale. La risoluzione di cui al periodo precedente è subordinata alla preventiva comunicazione all'ANAC, cui spetta la valutazione in merito all'eventuale prosecuzione del rapporto contrattuale, al ricorrere delle condizioni di cui all'art. 32 del decreto-legge 90/2014 convertito in legge 114 del 2014.

12. Il Concessionario è consapevole e dichiara di accettare che la presente Convenzione sarà risolta di diritto ai sensi di quanto previsto dall'art. 1456 del codice civile nel caso in cui dovesse intervenire, anche in corso di esecuzione contrattuale, un provvedimento interdittivo ai sensi e per gli effetti della disciplina antimafia di cui al decreto legislativo n. 152 del 2011 e successive modifiche come indicato nelle premesse.

## Articolo 15
## TUTELA DEI LAVORATORI

1. Il Concessionario si impegna al rispetto delle norme applicabili in materia di lavoro (compreso il rispetto della contrattazione collettiva applicabile), previdenza, antinfortunistica e radioprotezione e garantisce che siano applicate ai propri dipendenti e collaboratori condizioni retributive non inferiori a quelle dei contratti collettivi nazionali, ove applicabili, in base alle categorie ed al luogo di svolgimento delle attività.

2. In particolare, il Concessionario applica al proprio personale dipendente, impiegato nell'esecuzione della Concessione e dei Contratti, il contratto collettivo nazionale e territoriale in vigore per il settore e per la zona, stipulato dalle associazioni dei datori e dei prestatori di lavoro comparativamente più rappresentative sul piano nazionale, e il cui ambito di applicazione sia strettamente connesso con le attività oggetto della Concessione.

3. Ai sensi dell'art. 30 del Codice, in caso di inadempienza contributiva risultante dal DURC, relativo a personale dipendente del Concessionario o dei soggetti titolari di subappalti e cottimi, di cui all'articolo 174 del Codice, impiegato nell'esecuzione della Concessione e/o del Contratto, il Concedente e/o l'Amministrazione Utente trattiene dal certificato di pagamento l'importo corrispondente all'inadempienza per il successivo versamento diretto agli enti previdenziali e assicurativi.

4. In caso di ritardo nel pagamento delle retribuzioni dovute al personale, di cui al comma 2 del presente articolo, il RUP invita per iscritto il soggetto inadempiente, e, in ogni caso, il Concessionario, a provvedervi entro i successivi 15 (quindici) giorni. Ove non sia stata contestata, formalmente e motivatamente, la fondatezza della richiesta entro il termine sopra assegnato, il Concedente e/o l'Amministrazione utente paga direttamente ai lavoratori le retribuzioni arretrate, detraendo il relativo importo dalle somme dovute al Concessionario ovvero dalle somme dovute al subappaltatore inadempiente, nel caso in cui sia previsto il pagamento diretto, ai sensi dell'articolo 174 del Codice e previa autorizzazione del Concedente, in funzione anche di coordinamento delle obbligazioni di Concessione e verifica delle condizioni di applicabilità della norma appena citata.

5. In ogni caso, sull'importo netto del corrispettivo a carico del Concedente e/o dell'Amministrazione Utente è operata, in relazione a ciascuna delle scadenze di versamento dei Corrispettivi per il Servizio, una ritenuta dello 0,50% (zero virgola cinquanta per cento). Le

ritenute possono essere svincolate in sede di liquidazione finale, dopo l'approvazione da parte del Concedente e/o dell'Amministrazione Utente del certificato o verbale di Verifica di Conformità, di cui all'art. 39 della Convenzione, previo rilascio del DURC.

6. Ai sensi dell'art. 28 del decreto legislativo n. 81/08, è stato redatto, ed è allegato alla Convenzione (Allegato K) il DUVRI Contrattuale, cui il Concessionario deve attenersi nello svolgimento delle proprie attività.

7. Il Concessionario si impegna, altresì, al rispetto degli obblighi in materia ambientale, sociale e del lavoro, stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali, ai sensi dell'art. 30 del Codice ed elencate nell'Allegato X al medesimo Codice.

## Articolo 16
## OBBLIGAZIONI DEL CONCEDENTE

1. Il Concedente si impegna ad approvare il Piano operativo dell'infrastruttura entro 30 (trenta) giorni dalla presentazione del Piano stesso da parte del Concessionario nonché a compiere gli adempimenti necessari per la Verifica di Conformità nei termini di cui alla presente Convenzione.

2. Il Concedente si impegna a compiere, con la propria struttura interna, attività di promozione al fine di far usufruire del Servizio il maggior numero di Amministrazioni Utenti nel più breve tempo possibile, anche in considerazione delle risorse messe a disposizione delle stesse Amministrazioni dal Piano nazionale di ripresa e resilienza (PNRR), Missione 1, Componente 1, Asse 1.

## Articolo 17
## ULTERIORI ATTIVITÀ DEL CONCEDENTE

1. Il Concedente si riserva il diritto di verificare in ogni momento l'esecuzione delle prestazioni contrattuali e di richiedere al Concessionario l'elaborazione di *report* specifici anche in formato elettronico e/o in via telematica, da inviare entro 15 (quindici) giorni dalla data di richiesta, pena l'applicazione delle penali di cui al successivo art. 21 della presente Convenzione.

2. Le risultanze delle attività di verifica e controllo di cui al presente articolo saranno comunicate al Comitato di cui all'art. 12 della presente Convenzione perché siano eventualmente discusse in contraddittorio in seno al Comitato, sia laddove si presentino delle criticità, perché si individuino in modo collaborativo le misure adatte al loro superamento, sia perché possano formare oggetto di conoscenza e miglioramento della *performance* laddove mettano in luce elementi positivi suscettibili di ulteriore implementazione o estensione.

## SEZIONE IV – AVVIAMENTO

### Articolo 18
### PIANO FABBISOGNI, PROGETTO DEL PIANO DEI FABBISOGNI, MIGRAZIONE

1. Le Amministrazioni Utenti potranno stipulare il Contratto entro 30 (trenta) mesi dalla sottoscrizione della Convenzione salva proroga di quest'ultimo termine concordata tra Concedente e Concessionario. A tal fine, le Amministrazioni Utenti dovranno fornire al Concessionario, che dovrà collaborare alla sua stesura, il Piano dei Fabbisogni che contiene l'elenco aggiornato del perimetro IT coinvolto nell'affidamento dei Servizi, con indicazione delle modalità richieste (*Housing, Hosting, IaaS e Cloud*), nell'ambito di quanto previsto dal Catalogo dei Servizi e secondo i termini e le condizioni di cui al Capitolato Servizi. Tale elenco fornirà gli elementi per poter identificare l'insieme dei Servizi e le relative modalità di fornitura alla singola Amministrazione Utente, i quali costituiranno l'oggetto del Contratto.

2. Il Concessionario entro 60 (sessanta) giorni dalla ricezione del Piano dei Fabbisogni dovrà trasmettere all'Amministrazione il relativo Progetto del Piano dei Fabbisogni che deve contenere almeno le seguenti sezioni:

   a) "Descrizione dei Servizi" con il dettaglio, per ciascun servizio, di:

   - identificativo del servizio;
   - configurazione (ove applicabile);
   - quantità;
   - costi;
   - impegno delle eventuali risorse professionali previste;

   b) "Piano di Migrazione di Massima", comprensivo dei suoi allegati.

3. È fatta salva la possibilità per l'Amministrazione Utente di presentare osservazioni al Progetto del Piano dei Fabbisogni, nel termine di 10 (dieci) giorni dalla ricezione, con esclusivo riferimento alle modalità di esecuzione delle attività di Migrazione e alle relative tempistiche, dettate da specifiche oggettive esigenze dell'Amministrazione stessa.

4. Le osservazioni dell'Amministrazione Utente saranno discusse in buona fede, sia laddove evidenzino criticità, perché si individuino in modo collaborativo le misure adatte al loro superamento, sia perché possano formare oggetto di conoscenza e miglioramento del progetto di dettaglio, laddove mettano in luce elementi positivi suscettibili di ulteriore implementazione o estensione.

5. Tenuto conto delle risultanze del dialogo di cui al comma 4 del presente articolo, il Concessionario provvederà alle conseguenti modifiche al Progetto del Piano dei Fabbisogni, nei 10 (dieci) giorni successivi alla ricezione delle osservazioni.

6. Nel caso in cui l'Amministrazione non provveda all'accettazione del Progetto del Piano dei Fabbisogni, così come emendato ai sensi del comma precedente, entro i successivi 10 (dieci) giorni, della questione sarà investito il Comitato di controllo costituito ai sensi della Convenzione.

7. Il Progetto del Piano dei Fabbisogni si intende in ogni caso accettato con la stipula del Contratto, di cui sarà un allegato.

8. Lo schema del Contratto tra Concessionario ed Amministrazioni Utenti è allegato alla Convenzione a formarne parte integrante.

## SEZIONE V - FORZA MAGGIORE E SOSPENSIONE DELLE ATTIVITÀ

### Articolo 19
### FORZA MAGGIORE E SOSPENSIONE DELLE ATTIVITÀ

1. Qualora si verifichi un qualsiasi evento di Forza Maggiore, la Parte che non può adempiere a causa di tale evento ne deve dare immediata comunicazione scritta all'altra Parte e/o all'Amministrazione Utente, con le modalità di cui all'art. 40 della Convenzione, descrivendo l'evento e indicando la prevedibile durata.

2. Fermo restando quanto sopra, qualora, in seguito a un evento di Forza Maggiore, o altro evento non imputabile al Concessionario, quest'ultimo non sia in grado di prestare, in tutto o in parte, il Servizio, il Concessionario deve fornire al Concedente ed alla Amministrazione Utente interessata, nell'informativa di cui al comma 1 del presente articolo, anche la descrizione delle prestazioni facenti parte del Servizio, o delle parti di esse, che non possono essere eseguite a causa di tale evento, nonché di quelle che possono essere eseguite, seppure parzialmente.

3. Nel caso di un evento di Forza Maggiore che determini una sospensione del Servizio, parziale, e/o totale per un periodo fino a 45 (quarantacinque) giorni, il Concessionario avrà diritto ad un'automatica proroga del termine di gestione del Servizio per un periodo pari a quello della sospensione. Qualora, invece, la sospensione si protragga per oltre 45 (quarantacinque) giorni e fino a 180 (centottanta) giorni, il Concessionario potrà anche richiedere la rideterminazione delle condizioni di Equilibrio Economico Finanziario, con le modalità di cui all'art. 11 della Convenzione, qualora ne ricorrano i presupposti.

   In caso di Forza Maggiore protratta per più di 180 (centottanta) giorni, ciascuna delle Parti può richiedere la risoluzione della Convenzione e/o dei Contratti, ai sensi dell'art. 1463 Cod. Civ. e, in tal caso, si applicano le previsioni degli artt. 35 e 36 della Convenzione e/o del Contratto.

4. In ogni caso di sospensione della Concessione, in coerenza con quanto disposto al presente articolo, resta definito che il Concessionario avrà diritto ad un'automatica proroga del termine di gestione del Servizio per un periodo pari a quello della sospensione. Qualora, invece, la sospensione si protragga per oltre 45 (quarantacinque) giorni e fino ai 180 (centottanta) giorni, il Concessionario potrà anche richiedere la rideterminazione delle condizioni di Equilibrio Economico Finanziario, con le modalità di cui all'art. 11 della Convenzione, qualora ne ricorrano i presupposti. Ove, invece, la sospensione sia protratta per più di 180 (centottanta) giorni, ovvero l'evento che determina la sospensione comporti l'oggettiva impossibilità definitiva per il Concessionario di adempiere alle proprie obbligazioni, ciascuna delle Parti può richiedere la risoluzione della Convenzione e/o dei Contratti, ai sensi dell'art. 1463 Cod. Civ. e, in tal caso, si applicano le previsioni degli artt. 35 e 36 della Convenzione e/o dell'art. 20 del Contratto con l'Amministrazione Utente.

## SEZIONE VI - CORRISPETTIVI E PENALI

### Articolo 20
### LIVELLI DI SERVIZIO

1. Le prestazioni che il Concessionario deve eseguire, nell'ambito del Servizio, devono garantire il rispetto dei Livelli di Servizio ("LS" o "SLA"), descritti nell'Allegato H – "Indicatori di Qualità".

2. Le modalità di erogazione delle prestazioni di cui all'articolo 5 e all'Allegato L sono descritte negli Allegati A "Capitolato Tecnico e relative Annessi – Capitolato Servizi" e B "Offerta Tecnica". La specificazione degli inadempimenti che comportano, relativamente alle attività oggetto della presente Convenzione, l'applicazione delle penali, nonché l'entità delle stesse, sono disciplinate nell'Allegato H – "Indicatori di Qualità".

## Articolo 21
## PENALI

1. Il ritardato, inadeguato o mancato adempimento delle obbligazioni di cui alla presente Convenzione che siano poste a favore del Concedente, importa l'irrogazione di penali.

   Egualmente, il ritardato, inadeguato o mancato adempimento delle obbligazioni che siano poste a favore delle Amministrazioni Utenti, importa l'irrogazione di penali disciplinate dai Contratti.

2. In considerazione di quanto previsto dall'art. 113-*bis*, comma 4, del Codice l'ammontare complessivo delle penali nel limite massimo del 10% (dieci per cento) dell'ammontare netto contrattuale, fermo il risarcimento degli eventuali maggiori danni, anche ai fini della risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima, è dato dalla somma delle penali che il Concessionario sopporterà in relazione alle obbligazioni poste a favore del Concedente e delle penali che il Concessionario sopporterà in relazione alle obbligazioni poste a favore delle Amministrazioni Utenti e previste dal Contratto.

3. La richiesta e/o il pagamento delle penali non esonera in nessun caso il Concessionario dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

4. È applicata una penale di € 150.000,00 (euro centocinquantamila/00), per ogni giorno di ritardo sui tempi offerti in sede di Gara per la disponibilità dell'Infrastruttura di cui al criterio ID 10 della tabella 5 del paragrafo 18.1 del disciplinare di Gara (*vedasi altresì matrice dei rischi di cui all'allegato G - voce "rischio di progettazione, predisposizione e allestimento*").

## Articolo 22
## PENALI DEL CONCEDENTE

1. In ipotesi di ritardato adempimento imputabile al Concessionario delle obbligazioni poste a favore del Concedente, fermo restando quanto disciplinato nell'Allegato H – "Indicatori di Qualità", il Concessionario sopporterà una penale giornaliera pari allo 0,3 (zero virgola tre) per mille dell'ammontare netto contrattuale delle obbligazioni rese in favore del Concedente per la realizzazione dell'Infrastruttura, vale a dire una penale giornaliera di Euro 4.800,00 (quattromilaottocento/00).

2. Il ritardato, inadeguato o mancato adempimento delle obbligazioni di cui alla presente Convenzione che siano poste a favore del Concedente deve essere contestato dal RUP nella sede del Comitato di Controllo. .

3. La contestazione deve avvenire con forma scritta e motivata ed opportunamente quantificata entro 8 (giorni) dall'evento o dalla sua conoscibilità.

   Laddove il Concessionario non contesti l'applicazione della penale a favore del Concedente, il Concessionario provvederà, entro e non oltre 60 (sessanta) giorni, a corrispondere al Concedente la somma dovuta; decorso inutilmente il termine di cui al presente comma, il Concedente potrà provvedere ad incassare le garanzie nei limiti dell'entità della penale.

   A fronte della contestazione della penale da parte del Concessionario, il Comitato di Controllo promuoverà un tentativo di conciliazione, assegnando a Concedente e Concessionario un termine comune per la presentazione in forma scritta delle proprie ragioni e della documentazione rilevante. Ad esito del contraddittorio scritto, il Comitato di Controllo tenterà la conciliazione di Concessionario e Concedente in seduta appositamente convocata. A fronte della mancata conciliazione tra le Parti il RUP irrogherà la penale e, salvo lo spontaneo pagamento da parte del Concessionario, pur senza che ciò corrisponda ad acquiescenza, incamererà la garanzia entro i limiti della penale. Resta fermo il diritto del Concessionario di contestare la penale iscrivendo riserva o agendo in giudizio per la restituzione.

4. Una volta che, in ragione delle penali irrogate dal Concedente, sia superato il limite massimo delle penali di cui all'art. 113-*bis*, comma 4, del Codice, è facoltà del Concedente risolvere la presente Convenzione.

## Articolo 23
## PENALI DELL'AMMINISTRAZIONE UTENTE

1. La ritardata, inadeguata o mancata prestazione dei Servizi a favore dell'Amministrazione Utente è oggetto delle penali previste dal relativo Contratto, che sono definite in termini oggettivi in relazione a quanto dettagliato all'Allegato H – "Indicatori di Qualità" .

2. In ipotesi di ritardato adempimento imputabile al Concessionario delle obbligazioni poste a favore dell'Amministrazione Utente, il Concessionario sopporterà una penale giornaliera definita nell'Allegato H – "Indicatori di Qualità" ai sensi di quanto specificato nel relativo Contratto.

## Articolo 24
## CORRISPETTIVI, PERIODICITÀ DEI PAGAMENTI E FATTURAZIONE

1. I Corrispettivi per il Servizio, determinati sulla base delle previsioni di cui al Capitolato Servizi, in applicazione dei Prezzi Offerti, sono versati dall'Amministrazione Utente al Concessionario, con cadenza bimestrale posticipata, a partire dalla data di avvio dei Servizi, secondo i termini previsti dal Contratto. Si precisa che i suddetti Corrispettivi e, in generale, ogni importo definito nella presente Convenzione o nei suoi allegati sono da intendersi oltre IVA, se dovuta.

2. Fermo restando quanto previsto dall'art. 30, commi 5, 5-*bis* e 6 del Codice, in relazione al caso di inadempienze contributive o retributive, e relative trattenute, i pagamenti avvengono dietro

presentazione di fattura fiscale, con modalità elettronica, nel pieno rispetto degli obblighi di tracciabilità dei flussi finanziari, di cui all'art. 3, legge 13 agosto 2010, n. 136 e successive modificazioni o integrazioni, mediante bonifico bancario sul conto [·] o, fermo il rispetto delle norme sulla tracciabilità dei flussi finanziari, su altro conto corrente intestato al Concessionario ed indicato nel Contratto, e previa indicazione di CIG nella causale di pagamento. A tal fine, il Concessionario indica nel Contratto i soggetti abilitati a operare sul conto corrente bancario.

3. Ai fini della fatturazione elettronica, ai sensi del Decreto Ministeriale 3 aprile 2013, n. 55 e successive modificazioni o integrazioni, il codice identificativo univoco dell'ufficio destinatario della fattura è indicato nel Contratto.

4. Il pagamento è effettuato entro 30 (trenta) giorni dalla data in cui è emessa la fattura. Alla scadenza del predetto termine, in mancanza del pagamento, si applicano le disposizioni di legge.

### Articolo 25
### SVINCOLO DELLE GARANZIE

1. Ove il Contratto lo preveda le Amministrazioni Utenti procedono allo svincolo delle garanzie prestate dal Concessionario, come disciplinate dagli artt. 26 e 27 della Convenzione, successivamente alla Verifica di Conformità, ai sensi dell'art. 39 della Convenzione.

## SEZIONE VII - GARANZIE E ASSICURAZIONI

### Articolo 26
### GARANZIA DEFINITIVA

1. Le Parti danno atto che il Concessionario ha provveduto a costituire la garanzia definitiva, di cui agli artt. 103 e 183, comma 13 del Codice, secondo lo schema tipo 1.2 del DM 19 gennaio 2018, n. 31 ("DM **Garanzie**"). La mancata prestazione delle garanzie conduce alla conseguenza della risoluzione per inadempimento per come disciplinata dall'art. 33, comma 2, lett. *d*) della presente Convenzione.

2. Il Concedente, in relazione agli artt. 103 e 183, comma 13 del Codice, riconosce che l'ammontare della garanzia definitiva di cui al presente comma corrisponde al 52,20% (cinquantadue virgola venti per cento del valore complessivo delle prestazioni che, a questi fini, si assumono equivalenti all'ammontare degli investimenti previsti nel PEF prodotto dall'operatore economico aggiudicatario, pari ad € 313.457.176,20. La predetta garanzia è stata ridotta del 20% sulla base di quanto previsto dall'art. 103 del Codice in virtù del possesso, da parte del Concessionario, della certificazione ISO 14001 ed è di conseguenza pari al 41,76% del valore degli investimenti sopra riportato per un importo totale pari a € 130.899.716,82.

   A beneficio di maggiore chiarezza, il Concedente riconosce che l'ammontare della garanzia definitiva si compone della garanzia prestata a favore del Concedente in relazione alle prestazioni rese in suo favore, dettagliate all'art. 14, comma 2.1., e delle garanzie definitive prestate nei singoli Contratti con le Amministrazioni Utenti, con riferimento alle prestazioni dettagliate all'art. 14, comma 2.2, e nel Contratto.

   Più in particolare, a garanzia delle obbligazioni contrattuali assunte nei confronti del Concedente

con la stipula della Convenzione il Concessionario ha prestato garanzia definitiva, rilasciata il giorno 24.08.2022 dalla società Euler Hermes S.A. sita in Roma, Via Raffaele Matarazzo, 19 - 00139, iscritta al n. 1.00099 nell'elenco IVASS, avente numero 2618257 di importo pari ad € 130.899.716,82 = (euro centotrentamilioniottocentonovantanovemilasettecentosedici/82).

3. La garanzia definitiva prestata in favore del Concedente opera a far data dalla sottoscrizione della Convenzione e dovrà avere validità almeno annuale da rinnovarsi, pena l'escussione, entro 30 (trenta) giorni dalla relativa scadenza per tutta la durata della Concessione. Allo stesso modo, in relazione ai singoli Contratti, opereranno le garanzie definitive concesse alle Amministrazioni Utenti.

4. Sia la garanzia definitiva a favore del Concedente che quelle previste dai Contratti con le Amministrazioni Utenti cessano di avere efficacia dalla data di attestazione, in qualunque forma, di regolare esecuzione delle prestazioni e vengono progressivamente svincolate in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80 (ottanta) per cento dell'iniziale importo garantito secondo quanto stabilito all'art. 103, comma 5, del Codice. Lo svincolo è automatico, senza necessità di nulla osta del Concedente, con la sola condizione della preventiva consegna all'istituto garante, da parte del Concessionario, degli stati di avanzamento o di analogo documento, in originale o in copia autentica, attestanti l'avvenuta esecuzione. In ogni caso lo svincolo avverrà periodicamente con cadenza trimestrale a seguito della presentazione della necessaria documentazione al Concedente o all'Amministrazione Utente secondo quanto di competenza.

5. Sia la garanzia definitiva a favore del Concedente che quelle previste dai Contratti con le Amministrazioni Utenti, laddove il loro ammontare dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, dovranno essere reintegrate dal Concessionario entro il termine di 45 (quarantacinque) giorni lavorativi dal ricevimento della relativa richiesta effettuata dal Concedente o dall'Amministrazione Utente.

6. Sia la garanzia definitiva a favore del Concedente che quelle previste dai Contratti con le Amministrazioni Utenti, sono integrate dal Concessionario a fronte dell'ampliamento del valore dei Servizi dedotti in Contratto nel corso dell'efficacia di questo, ovvero di estensione della durata della Convenzione e/o del Contratto.

## Articolo 27
## POLIZZE ASSICURATIVE

1. Ai sensi dell'art. 103 del Codice, il Concessionario si impegna a stipulare idonee polizze assicurative, a copertura delle attività oggetto della Concessione. In particolare, ferme restando le coperture assicurative previste per legge in capo agli eventuali professionisti, di cui il Concessionario si può avvalere nell'ambito della Concessione, il Concessionario ha l'obbligo di stipulare:

a. una polizza assicurativa a copertura della responsabilità civile professionale dei tecnici a vario titolo incaricati per la realizzazione e implementazione dell'Infrastruttura, avente decorrenza dalla data di stipula della Convenzione e, in ogni caso, dalla data di inizio delle prestazioni ivi comprese quelle a favore delle Amministrazioni Utenti;

b. una polizza assicurativa a favore del Concedente a copertura dei danni che possano derivare all'Infrastruttura oggetto di devoluzione a fine Concessione con massimale non inferiore al valore residuo dell'Infrastruttura stimato da PEF; una polizza assicurativa a favore delle singole Amministrazioni Utenti, a copertura dei danni che possano derivare dalla prestazione dei Servizi, con validità ed efficacia a far data dalla sottoscrizione del singolo Contratto con l'Amministrazione Utente.

c. una polizza assicurativa Polizza RCT/RCO, con un capitale assicurato, per ogni sinistro, pari a € 5.000.000,00 (cinque milioni), da rivalutarsi ogni 5 anni in relazione alla svalutazione monetaria intervenuta dalla stipula della presente Convenzione, a garanzia di ogni danno causato agli utenti, ai terzi ed alle cose nello svolgimento dell'attività di gestione dell'Infrastruttura. In particolare, la polizza è posta a garanzia del rischio da responsabilità civile derivante dall'esercizio dell'attività di gestione dell'Infrastruttura per eventuali danni agli utenti, ai visitatori, ai dipendenti, ai lavoratori, al personale distaccato dal Concedente, ed a tutti coloro che possono essere a vario titolo coinvolti per ragioni professionali o meno nella gestione o nella visita dell'infrastruttura.

2. Le suddette coperture assicurative, che devono recare l'espressa rinuncia alla rivalsa nei confronti del Concedente, devono in ogni caso contemplare:

- l'inclusione della responsabilità civile "personale" dei prestatori di lavoro del Concessionario, compresi gli addetti appartenenti a tutte le figure professionali previste ai sensi delle vigenti norme che regolano il mercato del lavoro, i soci lavoratori di cooperative, i volontari, i tirocinanti, gli stagisti e compresi altresì altri soggetti al servizio, anche temporaneo, del Concessionario;

- l'estensione ai danni derivanti al Concedente e a terzi da incendio di cose del Concessionario o dallo stesso detenute.

Nella garanzia RCO devono essere comprese tutte le figure di prestatori di lavoro previste dalle vigenti normative in materia di lavoro, che svolgono la propria attività al servizio del Concessionario. La garanzia deve comprendere anche l'estensione alle malattie professionali.

## Articolo 28
## GARANZIE DEL CONCESSIONARIO PER I FINANZIATORI

1. Il Concedente prende atto ed accetta sin d'ora l'eventuale costituzione da parte del Concessionario in favore dei Finanziatori, di pegni su azioni del Concessionario e di garanzie sui crediti che verranno a maturazione in forza della Convenzione e dei singoli Contratti, nei confronti del Concedente e delle Amministrazioni Utenti.

2. In ogni caso, da tale accettazione non potranno derivare a carico del Concedente e/o delle Amministrazioni Utenti nuovi o maggiori oneri rispetto a quelli derivanti dalla presente Convenzione e/o dai Contratti e, con riferimento alla cessione dei, ovvero al pegno sui, crediti del Concessionario, lo stesso Concedente e/o le Amministrazioni Utenti potranno opporre al cessionario/creditore pignoratizio tutte le eccezioni opponibili al Concessionario in base alla Convenzione e/o ai singoli Contratti.

3. Il Concedente e/o l'Amministrazione Utente si impegnano a cooperare, per quanto di loro competenza, affinché siano sottoscritti i documenti necessari a garantire il perfezionamento e/o l'opponibilità, ove necessario, delle garanzie costituire a favore dei Finanziatori, inclusi a mero titolo esemplificativo eventuali atti di accettazione della cessione dei, o del pegno sui, crediti derivanti dalla Convenzione e/o dai Contratti.

4. In ogni caso, il Concessionario si impegna a far sì che eventuali cessioni del credito siano disposte solo *pro-soluto* e subordinatamente all'accettazione del Concedente ove sia debitore ceduto.

## SEZIONE VIII - VICENDE DELLA CONCESSIONE

### Articolo 29
### SUBAPPALTO E AFFIDAMENTI I DEL CONCESSIONARIO

1. Il Concessionario, per l'affidamento a terzi di prestazioni che formano oggetto della Concessione, può procedere mediante contratti di subappalto a terzi nei limiti e con le modalità previste dall'art. 174 del Codice e dalla Documentazione di Gara nonché secondo quanto indicato nell'Offerta.

2. Il Concessionario può inoltre procedere alla conclusione con terzi di contratti non riconducibili al subappalto, inclusi i subcontratti, in conformità con le norme applicabili.

3. Le prestazioni eseguite dai soci del Concessionario, inclusi quelli subentrati successivamente, nonché dalle imprese ad essi collegate, ai sensi degli articoli 174, comma 2, e 184, comma 2, del Codice, non costituiscono affidamenti a terzi.

### Articolo 30
### MODIFICA DELLA CONCESSIONE DURANTE IL PERIODO DI EFFICACIA

1. Fermo quanto previsto dall'art. 5, le variazioni dei termini e condizioni della Convenzione in costanza della stessa possono intervenire con il rispetto ed entro i limiti di cui all'art. 175 del Codice, ad esito del contraddittorio tra le Parti, redigendo apposito atto aggiuntivo alla presente Convenzione, dal quale risultino le nuove clausole e i nuovi prezzi, che diventeranno parte integrante della Convenzione.

   Resta chiarito fin d'ora che, sempre nel rispetto dell'art. 175 del Codice, saranno disposte con appositi atti aggiuntivi le varianti necessarie perché (i) sia assicurato alle Amministrazioni Utenti l'aggiornamento rispetto alle tecnologie di tempo in tempo rese disponibili sul mercato, secondo quanto disposto dall'art. 5, comma 4, numero *i*) della presente Convenzione, (ii) sia assicurata l'integrazione dei Servizi a favore delle Amministrazioni Utenti con la previsione di nuovi servizi,

non originariamente previsti dal Catalogo dei Servizi perché frutto dell'evoluzione tecnologica o gestionale, nonché dell'esperienza maturata nella fornitura dei Servizi, secondo quanto disposto dall'art. 5, comma 4, numero *ii*), della presente Convenzione (iii) sia disposto l'aggiornamento dei corrispettivi per i Servizi, modificati con la determinazione di nuovi prezzi in ragione di quanto deriva, fermo restando l'equilibrio economico finanziario e i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto, da quanto disposto dall'art. 5, comma 4, numeri *i*) e *ii*) della presente Convenzione.

Le modifiche del Servizio non possono avere l'effetto di modificare la natura delle prestazioni previste in Convenzione.

2. Fermo restando quanto stabilito nei precedenti commi del presente articolo, le Parti concordano che le variazioni di cui al comma 1 del presente articolo ed all'art. 5 della Convenzione danno luogo all'avvio della procedura di revisione del PEF Contrattuale, con applicazione dell'art. 11 della Convenzione.

3. Le Parti riconoscono che le eventuali modifiche temporanee nelle modalità di pagamento, dovute a eventi di Forza Maggiore non rientrano tra le variazioni contrattuali disciplinate dal presente articolo o dall'art. 175 del Codice.

## SEZIONE IX - CESSAZIONE DEL CONTRATTO

### Articolo 31
### EFFICACIA DEL CONTRATTO

1. La Convenzione è efficace dalla data della sua sottoscrizione.

### Articolo 32
### CAUSE DI RISOLUZIONE AUTOMATICA

1. La Concessione e/o il singolo Contratto cessano automaticamente nei casi disciplinati dall'art. 176 del Codice. A maggiore chiarimento le Parti si danno atto che avendo il Concessionario assunto il rischio di finanziamento ai sensi dell'art. 9, comma 1, lettera e) della presente Convenzione, il venire meno del Contratto di Finanziamento non determina di per sé una ipotesi di risoluzione automatica.

2. Nel caso di annullamento d'ufficio debbono essere corrisposti gli indennizzi di cui all'art. 176, comma 4, del Codice.

3. La risoluzione della Convenzione determina la risoluzione dei singoli Contratti a partire dalla data in cui si verifica la risoluzione della Convenzione, salvo comunque l'indennizzo di cui all'art. 176, comma 4, del Codice. In tal caso il Concessionario si impegna a porre in essere ogni attività necessaria per assicurare la continuità del Servizio in favore delle Amministrazioni Utenti secondo la disciplina di cui all'art. 37.

### Articolo 33
### RISOLUZIONE PER INADEMPIMENTO DEL CONCESSIONARIO

1. Ai sensi dell'art. 176, comma 7, del Codice, qualora la Concessione e/o il singolo Contratto siano risolti per inadempimento del Concessionario, trova applicazione l'art. 1453 Cod. Civ.

2. Il Concedente e/o le singole Amministrazioni Utenti possono dar luogo alla risoluzione della Convenzione e/o del Contratto, previa diffida ad adempiere, ai sensi dell'art. 1454 Cod. Civ., comunicata per iscritto al Concessionario, ai sensi dell'art. 40 della Convenzione, con l'attribuzione di un termine per l'adempimento ragionevole e, comunque, non inferiore a giorni 60 (sessanta), in caso di:

   a. riscontro di gravi vizi nella gestione del Servizio secondo quanto previsto dall'art. 176 del Codice;

   b. conclamata insolvenza del Concessionario, ovvero ove sia dichiarato il fallimento dello stesso;

   c. applicazione di penali da parte del Concedente, in relazione alle obbligazioni poste in suo favore, ai sensi dell'art. 21 della Convenzione, per un importo che supera complessivamente il 10% (dieci per cento) dell'importo contrattuale netto e/o, in relazione alla risoluzione dei

Contratti, il 10% (dieci per cento) del valore del singolo Contratto;

d. mancata attivazione, da parte del Concessionario, di una delle coperture assicurative, previste per legge e ai sensi della Convenzione, o mancato reintegro delle garanzie, ove le stesse si siano ridotte per qualsiasi causa, fermo restando il loro progressivo svincolo;

e. sentenza di condanna passata in giudicato dei soggetti di cui all'art. 80, comma 3 del Codice per i reati di cui all'art. 80, comma 1 del Codice;

f. violazione delle obbligazioni in materia di monitoraggio per come definite dalle Linee Guida ANAC n. 9, approvate dal Consiglio dell'Autorità con Delibera n. 318 del 28 marzo 2018, di attuazione del decreto legislativo 18 aprile 2016, n. 50, recanti «*Monitoraggio delle amministrazioni aggiudicatrici sull'attività dell'operatore economico nei contratti di partenariato pubblico privato*».

3. In caso di risoluzione per inadempimento del Concessionario, a quest'ultimo sarà dovuto il pagamento delle prestazioni regolarmente eseguite a favore delle Amministrazioni Utenti, nonché il rimborso da parte del Concedente dei costi sostenuti, direttamente o indirettamente, e non remunerati per la progettazione, predisposizione, setup o ammodernamento dell'Infrastruttura decurtati degli oneri aggiuntivi derivanti dallo scioglimento del contratto.

4. La risoluzione della Convenzione determina la risoluzione dei singoli Contratti a partire dalla data in cui si verifica la risoluzione della Convenzione. In tal caso il Concessionario si impegna a porre in essere ogni attività necessaria per assicurare la continuità del Servizio in favore delle Amministrazioni Utenti, fermo il pagamento del prezzo delle prestazioni che saranno rese alle Amministrazioni Utenti.

## Articolo 34
## SOSTITUZIONE DEL CONCESSIONARIO E SUBENTRO

1. Ai sensi dell'art. 176, commi 8 e ss. del Codice, in tutti i casi di inadempimento del Concessionario, che possano dare luogo alla risoluzione della Convenzione e/o del Contratto, al di fuori delle ipotesi di cui all'art. 37 che segue, il Concedente comunica per iscritto - con le modalità di cui all'art. 40 della Convenzione - al Concessionario e ai Finanziatori, l'intenzione di risolvere il rapporto contrattuale.

2. I Finanziatori, ivi inclusi i titolari di obbligazioni e titoli analoghi emessi dal Concessionario, entro 90 (novanta) giorni dal ricevimento della comunicazione, indicano un operatore economico, che subentri nella Concessione, avente caratteristiche tecniche e finanziarie corrispondenti, o analoghe, a quelle previste nella Documentazione di Gara, con riguardo allo stato di avanzamento della Concessione alla data del subentro.

3. L'operatore economico subentrante deve assicurare la ripresa dell'esecuzione della Concessione e l'esatto adempimento, originariamente richiesto al Concessionario sostituito, entro il termine indicato dal Concedente. Il subentro dell'operatore economico ha effetto dal momento in cui il Concedente e/o la singola Amministrazione Utente vi presta il consenso.

## Articolo 35

## RISOLUZIONE PER INADEMPIMENTO DEL CONCEDENTE E/O DELL'AMMINISTRAZIONE UTENTE O REVOCA DELLA CONCESSIONE E/O DEL CONTRATTO

1. La Concessione può essere revocata dal Concedente solo per inderogabili e giustificati motivi di pubblico interesse, che debbono essere adeguatamente motivati e comprovati, con contestuale comunicazione della revoca stessa al Concessionario, con le modalità di cui all'art. 40 della Convenzione, unitamente ai relativi motivi. In tal caso, il Concedente deve corrispondere al Concessionario le somme di cui al successivo articolo 36.

2. Allo stesso modo, le Amministrazioni Utenti potranno revocare i Contratti solo per inderogabili e giustificati motivi di pubblico interesse, che debbono essere adeguatamente motivati e comprovati e corrispondendo al Concessionario, ai sensi dell'art. 176, commi 4 e 5, del Codice, gli importi maturati dal Concessionario in ragione delle prestazioni rese, il ristoro dei costi sostenuti per la produzione di Servizi non ancora interamente prestati o non pagati, il ristoro dei costi e delle penali da sostenere in conseguenza della risoluzione o del recesso.

3. La Convenzione e/o il Contratto sono risolti per inadempimento del Concedente e/o della singola Amministrazione Utente secondo quanto previsto dall'art. 176 del Codice, a fronte del verificarsi dei casi previsti dalla stessa disposizione o per l'inadempimento delle obbligazioni previste dall'art. 16 della presente Convenzione.

4. L'efficacia della risoluzione della Convenzione e/o del singolo Contratto non si estende alle prestazioni già eseguite ai sensi dell'art. 1458 c.c..

5. L'efficacia della revoca della Convenzione e/o del singolo Contratto è subordinata al pagamento, da parte del Concedente e/o dell'Amministrazione Utente, degli importi previsti al successivo articolo della presente Convenzione e nel Contratto.

## Articolo 36

## EFFICACIA DELLA REVOCA E DELLA RISOLUZIONE E SOMME SPETTANTI AL CONCESSIONARIO

1. Qualora la Concessione sia risolta per inadempimento del Concedente non imputabile al Concessionario, ovvero sia revocata dal Concedente per motivi di pubblico interesse, al Concessionario spetta, ai sensi dell'art. 176, commi 4 e 5 del Codice, il pagamento delle somme relative:

   a) agli importi eventualmente maturati dal Concessionario ai sensi della Convenzione e dei Contratti;

   b) al ristoro dei costi sostenuti, direttamente o indirettamente, per la progettazione, predisposizione, setup o ammodernamento dell'infrastruttura in quanto non siano già stati interamente remunerati;

c) (i) al ristoro dei costi e delle penali da sostenere, in conseguenza della risoluzione, ivi inclusi gli oneri derivanti dallo scioglimento degli eventuali contratti di copertura del rischio di fluttuazione del tasso di interesse e dei contratti di collaborazione e/o lavoro subordinato a qualsivoglia titolo intrattenuti dal Concessionario; (ii) all'indennizzo a titolo di risarcimento del mancato guadagno, pari al 10% (dieci per cento) del valore attuale dei ricavi, risultanti dal PEF, per gli anni residui di gestione.

2. Al fine di quantificare gli importi, di cui al comma 1 del presente articolo, il Concedente e/o le singole Amministrazioni Utenti, per quanto di rispettiva competenza, in contraddittorio con il Concessionario e alla presenza del DEC, redigono apposito verbale, entro 30 (trenta) giorni successivi alla ricezione, da parte del Concessionario, del provvedimento di revoca della Concessione e/o del Contratto.

   Qualora tutti i soggetti coinvolti siglino tale verbale senza riserve, e/o contestazioni, i fatti e dati registrati si intendono definitivamente accertati, e le somme dovute al Concessionario devono essere corrisposte entro 30 (trenta) giorni successivi alla compilazione del verbale. In caso di mancata sottoscrizione la determinazione è rimessa all'arbitraggio di un terzo nominato dal Presidente del Tribunale di Roma.

3. Le somme corrisposte dal Concedente al Concessionario, di cui al comma 1 del presente articolo, sono destinate prioritariamente, salvi i privilegi di legge, al soddisfacimento dei crediti dei Finanziatori. Tali somme sono indisponibili, da parte del Concessionario, fino al completo soddisfacimento di detti crediti.

4. Per tutto quanto non specificato nel presente articolo, si rinvia integralmente all'art. 176 del Codice.

## Articolo 37
## RECESSO

1. In caso di sospensione del Servizio per cause di Forza Maggiore, ai sensi dell'art. 19 della Convenzione, protratta per più di 180 (centottanta) giorni, o nel caso in cui, entro un periodo di 180 (centottanta) giorni, non sia raggiunto un accordo tra le Parti in merito alle condizioni di Revisione, ai sensi dell'art. 11 della Convenzione, ciascuna delle Parti può esercitare il diritto di recedere dalla Convenzione.

2. Nei casi di cui al comma precedente del presente articolo, il Concedente deve, prontamente, corrispondere al Concessionario l'importo di cui all'art. 36 della Convenzione fatta eccezione per
   (a) l'indennizzo previsto al punto (ii) della lettera c) del comma 1 dell'articolo 36 medesimo e, con l'esclusione
   (b) nel caso in cui il recesso derivi dal mancato accordo all'esito della procedura di riequilibrio prevista dalla presente Convenzione diretta ad ottenere il ripristino degli Indicatori di Equilibrio, dei costi derivanti dallo scioglimento anticipato dei contratti di copertura del rischio di fluttuazione del tasso di interesse.

3. Nelle more dell'individuazione di un Concessionario subentrante, il Concessionario dovrà proseguire, laddove richiesto dal Concedente e/o dall'Amministrazione Utente, nella prestazione

del Servizio, alle medesime modalità e condizioni previste dalla Convenzione e/o dal Contratto. Laddove la prosecuzione del Servizio richieda ulteriori investimenti ovvero l'Amministrazione Utente li richieda o tali ulteriori investimenti conseguano ai Servizi richiesti, oppure il costo del Servizio ed in generale l'economicità della prestazione siano alterati rispetto alla redditività prevista dal PEF e realizzata in costanza di contratto, il Concessionario dovrà essere interamente rimborsato degli investimenti o degli extra-costi in questione entro 30 (trenta) giorni dalla loro realizzazione, ferma la facoltà del Concessionario di non porre in essere detti ulteriori investimenti ed interrompere immediatamente il Servizio e non prorogare l'esecuzione del Contratto, pur restando fermo il diritto a percepire il compenso conseguente ai Servizi resi fino a quel momento. Resta fermo, comunque, che la prosecuzione delle prestazioni non potrà eccedere il termine di 12 (dodici) mesi.

4. Inoltre, fermo restando quanto previsto al precedente comma del presente articolo, il Concessionario continuerà a gestire il Servizio alle medesime modalità e condizioni della Convenzione e/o del Contratto con le conseguenti obbligazioni del Concedente e/o dell'Amministrazione Utente fino alla data dell'effettivo pagamento delle somme, di cui al comma 2 del presente articolo.

## Articolo 38
## DEVOLUZIONE DELL'INFRASTRUTTURA E CLAUSOLA SOCIALE

1. Alla scadenza della Concessione, l'Infrastruttura progettata, predisposta ed allestita dal Concessionario sarà devoluta al Concedente o al gestore subentrante, a seconda delle determinazioni assunte dal Concedente. Si provvederà alla redazione di un verbale di restituzione dal quale risulti la consistenza e lo stato effettivo dell'infrastruttura alla data di cessazione della Concessione. Nel medesimo verbale, si darà atto della consegna da parte del Concessionario della predetta Infrastruttura, che passerà nella piena disponibilità del Concedente o del gestore subentrante di diritto, libera da vincoli o gravami di qualsivoglia natura, in ordinario stato di funzionamento, senza ulteriori formalità. Nel verbale saranno anche concordate con il Concessionario le misure necessarie a regolare i rapporti ancillari all'Infrastruttura – quali, a titolo solo esemplificativo, quelli concernenti la disponibilità degli immobili che ospitano l'Infrastruttura – secondo buona fede e nella prospettiva della massima apertura della concorrenza.

2. Per la devoluzione dell'Infrastruttura, al Concessionario sarà dovuto un rimborso pari al 90% del valore residuo dell'infrastruttura stessa, al netto dell'ammortamento degli investimenti intervenuto in ragione dell'esercizio delle attività di Concessione, per come desumibile dal bilancio del Concessionario, tenendo anche conto dell'obsolescenza tecnologica a cui la stessa è soggetta valutata dal Comitato di Controllo di cui all'articolo 12 che, per tale attività, può avvalersi anche della collaborazione di esperti in possesso di specifica ed elevata competenza in materia tecnico informatica. A tal fine fa espresso rinvio a quanto previsto dagli allegati B e G della presente convenzione nonché i relativi annessi.

3. L'integrale pagamento al Concessionario della somma di cui al precedente comma costituisce condizione essenziale per la devoluzione dell'Infrastruttura e per il subentro della gestione del Servizio.

4. Per maggiore chiarezza resta inteso che non sono parte dell'Infrastruttura progettata, predisposta

ed allestita dal Concessionario, ed oggetto di devoluzione gratuita gli immobili entro i quali essa è ospitata, i servizi ad essi correlati, i brevetti o i sistemi oggetto di protezione della proprietà intellettuale e, più in generale, tutto ciò che eccede il progetto di infrastruttura e le sue integrazioni di tempo in tempo approvate dal Concedente ed oggetto della Verifica di Conformità dell'Infrastruttura di cui all'articolo che segue.

5. Nelle more dell'individuazione di un gestore subentrante, esclusivamente nella misura in cui sia necessario a garantire esigenze di continuità dei servizi, il Concessionario è tenuto a proseguire la gestione alle medesime modalità e condizioni previste dalla Convenzione.

6. Il Concessionario ha l'obbligo di facilitare il subentro del Concedente o del nuovo Concessionario.

7. In caso di cambio di gestione della Concessione, il Concessionario subentrante provvederà all'assunzione del personale del Concessionario, in conformità alla normativa vigente.

## Articolo 39
## VERIFICA DI CONFORMITÀ DELL'INFRASTRUTTURA E DEI SERVIZI

1. Entro il trentaseiesimo (36°) mese dalla sottoscrizione della Convenzione, destinato alla progettazione, predisposizione ed allestimento della Infrastruttura, quest'ultima sarà oggetto di Verifica di Conformità, secondo le modalità fissate dalla presente Convenzione.

   Alla scadenza della Convenzione, o, comunque, al termine della Concessione, anticipata o estesa, per qualunque titolo o ragione di cui alla presente Convenzione o per legge, le integrazioni, variazioni ed aggiunzioni all'Infrastruttura dovute ai Contratti o a varianti della Convenzione saranno fatte oggetto di Verifica di Conformità dell'Infrastruttura con le stesse modalità previste dal presente articolo. Resta inteso che la Verifica di Conformità dell'Infrastruttura deve essere effettuata dal Concedente nel termine di 90 (novanta) giorni dalla sua ultimazione, come comunicata dal Concessionario in base all' art. 6, comma 2, primo capoverso della Convenzione.

2. Alla scadenza della Convenzione, o, comunque, al termine della Concessione, anticipata o estesa, per qualunque titolo o ragione di cui alla presente Convenzione o per legge, il Concedente procede, ai sensi dell'art. 102 del Codice, ad effettuare la Verifica di Conformità dei Servizi.

3. La Verifica di Conformità dei Servizi sarà svolta dalle Amministrazioni Utenti secondo le modalità che seguono, eventualmente integrate dalle previsioni dei Contratti e con gli adattamenti necessari quanto alle parti coinvolte. La Verifica di Conformità dei Servizi è finalizzata a certificare che il Servizio, in termini di prestazioni, obiettivi e caratteristiche tecniche, economiche e qualitative sia stato eseguito nel rispetto delle previsioni contrattuali, così come specificate nella Convenzione, nel Capitolato Servizi e nell'Offerta.

4. Le Verifiche di Conformità sono svolte sotto la supervisione del DEC ed alla presenza del RUP, dando avviso al Direttore del Servizio, attraverso le modalità previste dalla presente Convenzione, almeno 10 (dieci) giorni prima della data fissata per i controlli, affinché quest'ultimo, o un suo delegato, possa intervenire.

5. La Verifica di Conformità dei Servizi è effettuata nel termine di 120 (centoventi) giorni dall'ultimazione della prestazione.

6. All'esito di ciascuna Verifica di Conformità, si procede alla redazione di apposito verbale, sottoscritto da tutti i soggetti intervenuti, che è trasmesso al RUP per approvazione.

7. Il Concessionario mette a disposizione, a propria cura e spese, i mezzi necessari ad eseguire le Verifiche di Conformità.

8. Per quanto non espressamente previsto e disciplinato dal presente articolo, si rimanda a quanto stabilito dal Codice.

## SEZIONE X - ULTERIORI DISPOSIZIONI

### Articolo 40
### COMUNICAZIONI

1. Agli effetti della presente Convenzione, il Concessionario elegge domicilio in Roma, alla via Goito, numero 4.

2. Eventuali modifiche del suddetto domicilio devono essere comunicate per iscritto al Concedente e hanno effetto a decorrere dall'intervenuta ricezione della relativa comunicazione.

3. Tutte le comunicazioni previste dalla presente Convenzione devono essere inviate in forma scritta a mezzo lettera raccomandata A.R. oppure via PEC ai seguenti indirizzi:

   Se al Concedente, al seguente indirizzo: Roma, largo Pietro di Brazzà n. 86, all'attenzione del Capo Dipartimento per la trasformazione digitale, indirizzo PEC diptrasformazionedigitale@pec.governo.it.

   Se al Concessionario, all'indirizzo di cui al comma 1, all'attenzione del Legale Rappresentante dott. Massimo Mancini, indirizzo PEC pec@psn.telecompost.it.

4. Le dette comunicazioni sono efficaci dal momento della loro ricezione da parte del destinatario, certificata dall'avviso di ricevimento, nel caso di lettera raccomandata A.R., ovvero, nel caso di invio tramite PEC, dalla relativa ricevuta.

### Articolo 41
### NORME ANTICORRUZIONE E PROTOCOLLI DI LEGALITÀ

1. Il Concessionario, con la sottoscrizione della Convenzione, attesta, ai sensi e per gli effetti dell'art. 53, comma 16-*ter*, del d. lgs. 165/2001, di non aver concluso contratti di lavoro subordinato, o autonomo o, comunque, aventi ad oggetto incarichi professionali con *ex* dipendenti del DTD, che abbiano esercitato poteri autoritativi, o negoziali, per conto dello stesso DTD nei confronti del medesimo Concessionario nel triennio successivo alla cessazione del rapporto di pubblico impiego.

2. A tal fine, il Concessionario dà atto che il Concedente rimanda al Codice di Comportamento dei pubblici dipendenti di cui al Decreto del Presidente della Repubblica n. 63 del 2013 e s.m.i., per una sua più completa e piena conoscenza; il Concessionario si impegna ad osservare le disposizioni ivi contenute in quanto applicabili, assicurando un'ampia diffusione dello stesso ai propri dipendenti e collaboratori a qualsiasi titolo.

3. La violazione degli obblighi, di cui al presente articolo, costituisce causa di risoluzione della Convenzione per fatto del Concessionario. Il Concedente, verificata l'eventuale violazione, contesta per iscritto al Concessionario il fatto, assegnando un termine non superiore a 10 (dieci)

giorni lavorativi per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate, o risultassero non accoglibili, il Concedente procede alla risoluzione della Convenzione, ai sensi dell'art. 33 della Convenzione, fatto salvo il risarcimento dei danni.

## Articolo 42
## OBBLIGHI IN TEMA DI TRACCIABILITÀ DEI FLUSSI FINANZIARI

1. Il Concessionario assume tutti gli obblighi di tracciabilità dei flussi finanziari, per sé e per i propri subcontraenti, di cui all'art. 3, legge 13 agosto 2010, n. 136 e successive modificazioni o integrazioni, dandosi atto che, nel caso di inadempimento, la Convenzione, nonché qualsiasi subcontratto ad essa collegato e sottoposto alla previsione del presente articolo, si risolverà di diritto, *ex* art. 1456 Cod. Civ. A tal fine il Concessionario assume l'obbligo di inserire nei contratti con i suoi subcontraenti una specifica clausola relativa alla tracciabilità dei flussi finanziari in conformità all'art. 3, legge 13 agosto 2010, n. 136.

2. Il Concessionario dichiara di aver acceso presso l'Istituto Bancario Intesa San Paolo S.p.A. il conto corrente n. 1000/00136942, IBAN IT13V0306901000100000136942 quale conto corrente dedicato e si impegna a comunicare, ai fini della presente Convenzione e dei contratti di utenza, eventuali estremi identificativi di ulteriori conti correnti dedicati o variazioni di quello sopra riportato nonché i nominativi dei soggetti delegati ad operare sui predetti conti correnti.

## Articolo 43
## CONTROVERSIE E FORO COMPETENTE

1. Per tutte le controversie che dovessero insorgere nell'esecuzione della presente Convenzione è competente in via esclusiva l'Autorità Giudiziaria di Roma.

## Articolo 44
## TRATTAMENTO DEI DATI PERSONALI

1. In materia di trattamento dei dati personali, si rinvia alla Normativa Privacy e al GDPR, come vigenti e a quanto previsto dall'Allegato E alla presente Convenzione.

## Articolo 45
## REGISTRAZIONE E BOLLO

1. La Convenzione è soggetta a registrazione. Tutte le spese dipendenti dalla stipulazione della Convenzione sono a carico del Concessionario.

2. Il Concessionario si farà carico del pagamento degli oneri di bollo di cui alla presente Convenzione nella misura di € 16,00 ogni 4 facciate, allegati compresi. Si specifica che, anche dopo la sottoscrizione della presente Convenzione, l'Amministrazione concedente comunicherà, a consuntivo, gli oneri di bollo da versare che dovranno essere assolti dal Concessionario entro 5 giorni decorrenti dalla comunicazione dell'importo, in modalità virtuale, dandone prova al Concedente, secondo le disposizioni dell'Agenzia delle Entrate, ovvero mediante contrassegno. In caso di pagamento mediante contrassegno il Concessionario dovrà offrire prova di aver assolto

agli oneri tributari citati mediante la produzione di un documento, sottoscritto dal Concessionario, in cui siano specificati gli estremi della presente Convenzione ivi compresi CIG e CUP, il numero di contrassegni acquistati, il numero delle matricole dei contrassegni acquistati, ovvero in alternativa in cui i contrassegni siano apposti in originale e annullati.

## Articolo 46
## RINVIO AL CODICE, AL CODICE CIVILE E AD ALTRE DISPOSIZIONI DI LEGGE VIGENTI

1. Per quanto non espressamente disciplinato dalla Convenzione, trovano applicazione le disposizioni normative di cui al Codice e al Cod. Civ., e le altre disposizioni normative e regolamentari applicabili in materia.

2. Oltre all'osservanza di tutte le norme specificate nella Convenzione, il Concessionario ha l'obbligo di osservare tutte le disposizioni contenute in leggi, o regolamenti, in vigore o che siano emanati durante il corso della Concessione, di volta in volta applicabili.

**Dipartimento per la Trasformazione digitale**

ing. Mauro Minenna

MINENNA MAURO
PRESIDENZA
CONSIGLIO DEI
MINISTRI
24.08.2022 17:30:14
GMT+01:00

**Polo Strategico Nazionale S.p.A.**

dott. Massimo Mancini

Firmato digitalmente da:
MASSIMO MANCINI
Firmato il 24/08/2022 18:53
Seriale Certificato: 500
Valido dal 04/08/2022 al 03/08/2025
TI Trust Technologies QTSP CA

# CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO A

## CAPITOLATO TECNICO E RELATIVI ANNESSI – CAPITOLATO SERVIZI

**Oggetto dell'Allegato**

Il presente allegato è costituito dai seguenti annessi:

- Annesso 1: Progetto di fattibilità;
- Annesso 2: Specificazione delle caratteristiche del servizio e della gestione.

-

# Proposta per la realizzazione secondo il modello del Partenariato Pubblico Privato del Polo Strategico Nazionale

## Progetto di fattibilità

10 dicembre 2021

Rev. 2.0

TIM - Uso Interno - Tutti i diritti riservati.

**Sommario**


1 PREMESSA ..... 7
1.1 Presentazione del costituendo ATI ..... 12
1.1.1 TIM SpA ..... 12
1.1.2 CDP Equity S.p.A. ..... 13
1.1.3 Leonardo S.p.A. ..... 13
1.1.4 Sogei SpA ..... 15
1.2 Glossario ..... 15
1.3 Contesto tecnologico ..... 16
1.4 Presentazione di Progetto ..... 18
1.5 Oggetto della Fornitura ..... 24
1.5.1 La NewCo ..... 24
1.5.2 Tipologia di servizi erogati dalla NewCo PSN ..... 25
1.5.3 Servizi Core ..... 27
1.5.4 Servizi no Core ..... 27
1.6 Servizi erogati dai Soci ..... 27
1.7 Le Partnership della Compagine ..... 29
1.7.1 Google Cloud ..... 29
1.7.2 Microsoft Azure ..... 31
1.7.3 Oracle Cloud ..... 33
1.8 Certificazioni del Personale ..... 35
2 Servizi Offerti e Modalità di Erogazione ..... 37
2.1 Housing ..... 37
2.2 Hosting ..... 38
2.3 IaaS ..... 38
2.3.1 IaaS Private ..... 38
2.3.2 IaaS Shared ..... 39
2.4 PaaS Industry ..... 39
2.4.1 DBaaS ..... 39
2.4.2 PaaS IAM ..... 40
2.4.3 Big Data ..... 41
2.4.4 Artificial Intelligence ..... 43
2.5 BaaS e DRaaS ..... 44
2.5.1 BaaS: Golden copy protetta ..... 44
2.5.2 DRaaS ..... 46
2.6 CaaS ..... 46





TIM - Uso Interno - Tutti i diritti riservati.

2.7 Security ..... 46
2.7.1 DDOS Protection ..... 46
2.7.2 Servizi Professionali di Sicurezza ..... 48
2.7.2.1 Ambito di attività ..... 49
2.8 Refresh tecnologico ..... 50
2.9 Il ruolo dei CSP ..... 51
2.9.1 Public Cloud PSN Managed ..... 52
2.9.1.1 Il servizio ..... 54
2.9.1.2 Architettura fisica ..... 55
2.9.1.3 Ripartizione delle responsabilità ..... 56
2.9.1.4 Controllo della Rete ..... 56
2.9.1.5 Accesso verso l'esterno Frontend ..... 57
2.9.1.6 Encryption at-rest ..... 57
2.9.1.7 Gestione degli Aggiornamenti ..... 58
2.9.1.8 Modello di Supporto ..... 58
2.9.2 Secure Public Cloud ..... 58
2.9.2.1 Requisiti architetturali ..... 62
2.9.2.2 Architettura ..... 64
2.9.2.2.1 Cifratura e gestione delle chiavi (Key Management) ..... 65
2.9.2.2.2 Confidential Computing nell'ambito del PSN ..... 66
2.9.2.2.3 Servizio di Backup ..... 67
2.9.2.3 Governance ..... 68
2.9.3 Hybrid Cloud on PSN Site ..... 68
2.10 Multi Cloud ..... 72
2.10.1 Cloud Management Platform ..... 72
2.10.2 Security & Compliance in ambito Multi Cloud ..... 74
2.11 Servizio di Migrazione, Evoluzione e Professional Services ..... 74
2.11.1 Figure Professionali ..... 74
2.11.2 Migrazione ..... 77
2.11.3 Servizi di Evoluzione ..... 82
2.11.3.1 Re-platform ..... 82
2.11.3.2 Re-architect ..... 83
2.11.4 Professional Services ..... 85
2.11.5 Scenari di Migrazione ..... 87
2.11.6 Servizio opzionale di moving fisico ..... 90
2.12 Business & Culture Enablement ..... 90
**3 Sicurezza ..... 93**



TIM - Uso Interno - Tutti i diritti riservati.

3.1 Normative e standard di riferimento ..... 95
3.2 Personale e Competenze ..... 97
3.3 Processi di gestione della sicurezza ..... 98
3.4 Tecnologie e Best Practices ..... 99
3.5 Infrastructure Security ..... 100
3.6 Network security ..... 102
3.7 Data Security ..... 103
3.8 SOC ..... 103
3.8.1 End Point Protection ..... 104
3.8.2 Identity and Access Management ..... 104
3.8.3 Key Management ..... 105
3.8.4 Security Platform Management ..... 106
3.8.5 Security Policy Management & Enforcement ..... 107
3.8.6 Log Management ..... 107
3.8.7 Security Monitoring ..... 108
3.9 CERT ..... 108
3.9.1 Threat Hunting ..... 109
3.9.2 Threat intelligence & Infosharing ..... 109
3.9.3 Security Testing & Vulnerability Management ..... 110
3.9.4 Incident Response ..... 110
**4 Infrastruttura IT e Network ..... 111**
4.1 Apparati Hardware e software infrastrutturale ..... 111
4.1.1 High Level Design dell'architettura ..... 111
4.1.2 Componente server ..... 113
4.1.3 Componente storage ..... 115
4.1.4 Piattaforme software infrastrutturale ..... 115
4.1.5 Backup standard ..... 116
4.2 Network ..... 117
4.2.1 Componente Data Center Interconnection ..... 118
4.2.1.1 Il Backbone IP/MPLS ..... 118
4.2.1.2 Interfaccia Dense Wavelength Division Multiplexing ..... 118
4.2.1.3 Virtual Local Area Network ..... 118
4.2.1.4 Traffico ..... 119
4.2.2 Componente Wide Area Network ..... 119
4.2.2.1 Internet/Infranet Condivisa ..... 119
4.2.2.2 Profilatori di Traffico (Bandwindth management) ..... 119
4.2.2.3 IDS e APM ..... 120



TIM - Uso Interno - Tutti i diritti riservati.

4.2.2.4 Raccolta linee ..... 120
4.2.2.5 Virtual Private Network ..... 120
4.2.2.6 Connettività dedicata per la migrazione dati ..... 121
4.2.2.7 Hosting del router di terminazione ..... 121
4.2.3 Componente Local Area Network ..... 122
4.2.3.1 Apparati condivisi (locali in DC o estesi sui due DC) ..... 122
4.2.3.2 Apparati dedicati (locali in DC o estesi sui due DC) ..... 123
4.3 Facility ..... 124
4.3.1 Energia Elettrica ..... 124
**5 Caratteristiche Data Center ..... 126**
5.1 Determinazione caratteristiche del macrosistema Data Center ..... 126
5.1.1 Caratteristiche geografiche e topografiche ..... 128
5.1.2 Indipendenza connessioni elettriche ed impiantistiche ..... 128
5.2 Determinazione caratteristiche dei singoli Data Center ..... 128
5.2.1 Caratteristiche dimensionali del sito ..... 128
5.2.2 Caratteristiche topografiche ed ambientali ..... 129
5.2.3 Caratteristiche architettoniche e strutturali ..... 129
5.2.3.1 Sostenibilità energetica e certificazioni ..... 129
5.2.4 Infrastruttura elettrica ..... 131
5.2.4.1 Impianto di terra e protezione scariche atmosferiche ..... 131
5.2.4.2 Stazione di energia normale ..... 132
5.2.4.3 Stazione gruppi elettrogeni di emergenza ..... 132
5.2.4.4 Stazione UPS di continuità servizio ..... 132
5.2.4.5 Sistema pulsanti di sgancio di emergenza ..... 132
5.2.4.6 Rete di distribuzione primaria e secondaria ..... 133
5.2.4.7 Impianti di illuminazione ..... 133
5.2.4.8 Impianti di forza motrice dataroom ..... 133
5.2.4.9 Rete infrastruttura per manutenzione ..... 134
5.2.5 Infrastruttura climatizzazione ..... 134
5.2.5.1 Stazione di energia termica e frigorifera ..... 134
5.2.5.2 Efficienza Sistema di raffreddamento ..... 134
5.2.5.3 Sistema di controllo HVAC ..... 135
5.2.5.4 Reti di distribuzione idroniche e / o areauliche ..... 135
5.2.5.5 Rete di adduzione ..... 135
5.2.5.6 Rete di scarico acque nere ed acque bianche ..... 135
5.2.6 Impianti ausiliari e protezione incendio ..... 135
5.2.6.1 Impianto rivelazione fumi ed antiallagamento ..... 135



TIM - Uso Interno - Tutti i diritti riservati.

5.2.6.2 Impianto di diffusione sonora ai fini evacuazione ..... 136
5.2.6.3 Impianto di supervisione BEMS ..... 136
5.2.6.4 Impianto di estinzione incendio ..... 136
5.2.6.5 Sistema di deposito gasolio ..... 136
5.2.7 Impianti security ..... 137
5.2.7.1 Impianto controllo accessi ..... 137
5.2.7.2 Impianto antintrusione ..... 138
5.2.7.3 Impianto di videosorveglianza a circuito chiuso ..... 138
5.2.8 Architetture di rete ..... 139
5.2.8.1 Rete di distribuzione primaria ingresso provider ..... 139
5.2.8.2 Rete di distribuzione secondaria ..... 139
5.2.8.3 Locali Meet me room ..... 139



TIM - Uso Interno - Tutti i diritti riservati.

## Indice delle Figure

**Figura 1: Architettura Funzionale Golden Copy** ..... 45
**Figura 2: Rappresentazione dell'architettura di prevenzione del DDoS in presenza di attacchi** ..... 48
**Figura 3: Livelli di segregazione** ..... 55
**Figura 4: Isolamento fisico delle aree dedicate al PSN** ..... 56
**Figura 5: Distribuzione dei livelli di Operational Control per il Public Cloud PSN Managed** ..... 56
**Figura 6: Aree di intervento del PSN per il Public Cloud PSN Managed** ..... 57
**Figura 7: Architettura Secure Cloud Service** ..... 65
**Figura 8: Control Plane e architettura servizio** ..... 70
**Figura 9: Cloud Management Platform** ..... 73
**Figura 10: Esempio dashboard Sec&Compliance** ..... 74
**Figura 11: Flusso di Migrazione** ..... 78
**Figura 12: Cloud Maturity Model** ..... 79
**Figura 13: Livelli attuali e target del Cloud Capability Maturity Model** ..... 79
**Figura 14: Flusso processo di Re-platform** ..... 83
**Figura 15: Flusso processo di Re-architect** ..... 84
**Figura 16: Gestione della Sicurezza** ..... 100
**Figura 17: Connessione Data Center** ..... 118
**Figura 18: Ciclo virtuoso energia dei Data Center** ..... 130



TIM - Uso Interno - Tutti i diritti riservati.

# Lista delle revisioni

| Rev. | Data | Descrizione |
|---|---|---|
| 1.0 | 27/09/2021 | Prima versione del documento |
| 2.0 | 10/12/2021 | Seconda versione del documento.<br>Correzioni refusi e controllo ortografico.<br>Inseriti paragrafi:<br>1.4 Presentazione del Progetto<br>1.6 Servizi erogati dai Soci<br>1.7 Le Partnership della Compagine<br>1.8 Certificazioni del Personale<br>2.8 Refresh Tecnologico<br>2.11.6 Servizio opzionale di moving fisico<br>4.2.2.6 Connettività dedicata per la migrazione dati<br>4.2.2.7 Hosting del router di terminazione<br>5.2.3.1 Sostenibilità energetica e certificazioni |



TIM - Uso Interno - Tutti i diritti riservati.

# 1 PREMESSA

L'Agenzia per l'Italia Digitale è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato. In particolare, promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della Pubblica Amministrazione e nel rapporto tra questa, i cittadini e le imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

Per promuovere l'innovazione digitale nella Pubblica Amministrazione, l'Agenzia per l'Italia Digitale ha attivato un piano complessivo di trasformazione e digitalizzazione delle stesse, ponendo al centro del **modello** strategico la **componente infrastrutturale** (come descritto nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022) con l'obiettivo di **governare** la **trasformazione digitale**.

Le **direttrici evolutive** della componente infrastrutturale sono rappresentata da:

- La **realizzazione** del "**modello Cloud della Pubblica Amministrazione**" e l'applicazione del **principio Cloud First** con cui si intende **facilitare la migrazione dei Servizi delle Pubbliche Amministrazioni verso tale modello**
- La **razionalizzazione ed il consolidamento dei Data Center della Pubblica Amministrazione**, attraverso la progressiva **dismissione dei Data Center obsoleti e inefficienti**, con l'obiettivo di ridurre i costi di gestione delle infrastrutture IT in favore di maggiori investimenti in nuovi servizi digitali
- **L'adeguamento del modello di connettività al paradigma Cloud**, favorendo la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni e la diffusione della connettività nei luoghi pubblici a beneficio delle Pubbliche Amministrazioni, dei cittadini e delle imprese.

In questo contesto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce l'identificazione e la creazione di un nuovo **Soggetto** titolare di un insieme di infrastrutture IT con opportune caratteristiche, **qualificato** (con riferimento alla circolare dell'Agenzia per l'Italia Digitale n. 01 del 14 giugno 2019) **ad erogare alle Amministrazioni, in maniera continuativa e sistematica**:

- Servizi **Infrastrutturali (IaaS, PaaS, BaaS, CaaS)**
- Servizi di **Gestione della Sicurezza IT**
- Servizi di **Disaster recovery** e **Business Continuity**
- **Servizi Professionali** a supporto delle amministrazioni
- Servizi di **Assistenza** ai fruitori dei servizi erogati.

**Il progetto che il costituendo ATI realizzerà andrà a gestire l'infrastruttura IT (Data Center e Cloud)** con specifiche caratteristiche di affidabilità e sicurezza definite dall'Agenzia per l'Italia



TIM - Uso Interno - Tutti i diritti riservati.

Digitale, ospitando **le applicazioni che supportano l'erogazione di servizi alle Pubbliche Amministrazioni**. Il **Progetto** è destinato a tutti quei **servizi di rilevanza strategica e di interesse nazionale** per i quali non è consigliabile che la gestione dell'infrastruttura e dei dati venga delegata a terze parti.
Nel contesto sopra descritto, Il presente **Progetto di fattibilità** ha lo scopo di proporre i requisiti relativi alla fornitura di un Catalogo di Servizi in oggetto, in quantità, qualità e livelli di servizio adeguati che offra i **servizi** precedentemente **indicati** tramite Data Center **ad alta efficienza e sicurezza** alle **Pubbliche Amministrazioni, principalmente PAC di categoria B**.

La definizione di Pubbliche Amministrazioni Centrali e la classificazione di tale categoria B fa riferimento all'elenco delle Amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm (Legge di contabilità e di finanza pubblica) pubblicato da ISTAT all'interno della Gazzetta Ufficiale (fonte: ISTAT, elenco aggiornato al 30 settembre 2019). I Servizi essenziali sono quelli necessari al mantenimento delle attività economiche e sociali critiche.

Le **Pubbliche Amministrazioni di categoria** B (di seguito indicate come ***PAC*** di tipo B) sono quelle in possesso di Data Center con carenze strutturali e/o organizzative che impedisce loro di garantire la continuità dei Servizi.

Nel presente Capitolo è descritto il contesto in termini di caratteristiche applicative e di ambienti tecnologici e l'oggetto della fornitura, con lo scopo di definire i servizi richiesti; mentre nel **Capitolo 2** sono descritti i Servizi proposti.

Sono altresì indicati nel **Capitolo 3** le caratteristiche di Sicurezza e nel **Capitolo 4** i requisiti della Fornitura, ovvero i requisiti minimi del Servizio, se non diversamente specificato. Le modalità di esecuzione della Fornitura sono descritte nel documento di "*Specificazione delle caratteristiche del Servizio e della Gestione*".

Tutti i termini temporali (giorni, mesi, anni) indicati nel Progetto di fattibilità devono intendersi come "solari", ove non diversamente previsto; la fornitura è articolata in un unico lotto.

Il presente progetto ha l'obiettivo di fornire alla PA una serie di strumenti innovativi a servizio della transizione digitale. Il disegno complessivo si basa sui principi di **sicurezza**, **interoperabilità**, **trasparenza** e **portabilità** delle applicazioni e dei dati.
I pilastri su cui si basa il progetto sono quattro:

- la progettazione e gestione delle infrastrutture, a garanzia della sicurezza, dell'affidabilità, della disponibilità e della scalabilità dei servizi e delle applicazioni gestiti; il progetto prevede l'utilizzo di infrastrutture di Rete, Data Center e interconnessione focalizzate a garantire (by design) le funzionalità sopra riportate. La scalabilità, la disponibilità e la resilienza sono i principi di base delle infrastrutture proposte.
- Il sistema di governance amministrativo e tecnologico che assicura il controllo dei processi, dell'accesso ai dati e della protezione stessa rispetto ai principi di sovranità e di trasparenza. Saranno gestiti i modelli di rilascio di nuovi servizi e nuove tecnologie



TIM - Uso Interno - Tutti i diritti riservati.

seguendo una logica di controllo (sia in termini di sicurezza che di compliance) garantendo i principi di sovranità e di interoperabilità. Il progetto prevede la realizzazione di sistemi di gestione dei rilasci, di controllo degli accessi e di monitoraggio dei funzionamenti a supporto dei principi fondativi.

- Le tecnologie e le scelte architetturali improntate ai principi del multicloud, che permettano di interoperare e utilizzare le varie opzioni in modo agile e flessibile.
- L'inclusione della innovazione proveniente anche da soluzioni di Cloud Provider Internazionali (*Hyperscaler* o CSP), tutelando la titolarità, la sicurezza e la sovranità dei dati.

L'insieme di queste soluzioni ha lo scopo di:

- Offrire per tutta la durata del progetto soluzioni aggiornate in linea con le evoluzioni del mercato.
- La sicurezza del controllo dei dati, dell'accesso e della gestione in territorio italiano di tutta l'infrastruttura. I principi fondatori della proposta rimarranno costanti durante tutta la durata del progetto mentre le tecnologie via via adottate dovranno naturalmente seguire l'evoluzione ed il progresso tecnologico per rimanere sempre all'avanguardia in termini di efficacia e efficienza.
- La scalabilità e la varietà offerta da fornitori come gli *Hyperscaler.*
- L'accesso, reso sicuro e controllato, alle soluzioni *Hyperscaler* da parte del personale del PSN con impatto importante sulla formazione e la crescita delle competenze.
- Una apertura all'ecosistema del territorio con approccio API based per tutti i servizi previsti che permetterà la costruzione di nuovi scenari applicativi *cloud native*.

L'integrazione tra gli *Hyperscaler* e le soluzioni sovrane sarà guidata dai criteri di classificazione del dato. Ogni livello di classificazione che verrà definito dalle strutture competenti, per esempio dall'Agenzia per la Cybersicurezza Nazionale (ACN) potrà esser soddisfatto da una delle diverse soluzioni cloud rese disponibili:

- Soluzioni industry standard, per Hosting, Housing e Private cloud (IaaS, PaaS, CaaS, BaaS);
- Public Cloud PSN Managed, con controllo del software e della gestione;
- Hybrid Cloud on PSN Site;
- Secure Public Cloud - Criptazione dei dati con chiavi nell'esclusiva disponibilità del PSN, sistemi di backup dati e policy di sicurezza;



TIM - Uso Interno - Tutti i diritti riservati.

## 1.1 Presentazione del costituendo ATI

### 1.1.1 TIM SpA

TIM è una delle principali realtà ICT in Italia. Lavora per un'Italia sempre più digitale, per rispondere alle esigenze dei cittadini, delle imprese e delle istituzioni, anche nei momenti più difficili. Grazie a interventi realizzati su tutto il territorio, intensificati durante l'emergenza sanitaria per permettere al Paese di non fermarsi durante il lockdown, la fibra ottica di TIM ha connesso già a dicembre 2020 il 90% delle famiglie con linea fissa, con l'obiettivo di chiudere il digital divide in Italia entro il 2021, estendendo a tutti la possibilità di lavorare e studiare a distanza, navigare ad alta velocità e usufruire dei servizi TV e d'intrattenimento. Con l'ultrabroadband mobile LTE TIM viene raggiunto oltre il 99% della popolazione, mentre il 5G TIM raggiungerà la copertura nazionale entro il 2025/2026.

Al centro della strategia del Gruppo i clienti, quasi 100 milioni fra Italia e Brasile, a cui viene offerta una connettività convergente e sempre più ricca: insieme alle telecomunicazioni fisse e mobili anche TV, contenuti digitali per l'entertainment - video, musica, gaming - e soluzioni per la casa intelligente.

Numerosi gli investimenti nell'innovazione e nelle nuove frontiere del cloud ed edge computing, per offrire piattaforme e soluzioni innovative per la digitalizzazione delle imprese, dalle PMI alla grande industria, fino al mondo della pubblica amministrazione e della sanità. Diventano così sempre più smart realtà produttive e territori.

Da 18 anni TIM è presente nei principali indici di Sostenibilità, segno dell'impegno e dell'attenzione agli effetti delle proprie attività sulla comunità e sull'ambiente per una crescita sostenibile. Con il progetto Operazione Risorgimento Digitale - la prima grande scuola di Internet gratuita che opera grazie al contributo di 30 partner e con il sostegno di associazioni di categoria, terzo settore e importanti attori nel campo della innovazione sociale – vengono diffuse competenze digitali nel Paese. Un'iniziativa di cui hanno già fruito oltre 700.000 cittadini. E per quanto riguarda il footprint ambientale, l'azienda ha fissato l'obiettivo di diventare carbon neutral entro il 2030.
Il gruppo si avvale di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e pubbliche amministrazioni, anche in partnership con gruppi di primaria importanza: Noovle è la cloud company di TIM, leading cloud enabler e Centro di Eccellenza a supporto della trasformazione digitale delle aziende pubbliche e private italiane; Sparkle, primo fornitore di servizi wholesale internazionali in Italia e fra i primi 10 a livello globale, con una delle più grandi e avanzate reti al mondo; Olivetti è il polo digitale con focus sullo sviluppo di soluzioni Internet of things, Telsy opera nel settore della cybersecurity.

I numeri di TIM al 30 settembre 2020:

- 30,2 milioni le linee mobili in Italia
- 17 milioni gli accessi totali alla rete fissa
- 51,2 milioni le linee di TIM Brasil
- 52.480 il personale, di cui 42.827 in Italia



TIM - Uso Interno - Tutti i diritti riservati.

### 1.1.2 CDP Equity S.p.A.

CDP Equity S.p.A. (di seguito anche "CDP Equity" o la "Società"), costituita nel 2011 con il nome Fondo Strategico Italiano S.p.A. e rinominata in CDP Equity nel 2016, è un investitore paziente di lungo periodo e agisce secondo logiche di mercato. Gli interventi in settori strategici, con ritorni adeguati, sono connaturati alla sua missione di sostenere lo sviluppo del Paese. CDP Equity, che è una realtà controllata al 100% dal Gruppo CDP, opera acquisendo prevalentemente quote di minoranza in imprese di rilevante interesse nazionale, che siano in equilibrio economico-finanziario e presentino adeguate prospettive di redditività e sviluppo

CDP Equity investe in aziende di rilevante interesse nazionale, attraverso partecipazioni dirette e indirette. Mette a disposizione capitali per lo sviluppo a lungo termine di organizzazioni in settori chiave per favorire l'innovazione in tecnologie e infrastrutture indispensabili alla crescita del sistema Paese. Attraverso partecipazioni in fondi, e in fondi di fondi, supporta l'ecosistema imprenditoriale italiano. È inoltre un investitore di riferimento negli asset alternativi. In particolare, CDP Equity, che ad oggi ha investito complessivi 4,9 miliardi di euro, effettua:

- ***Investimenti Diretti*** intervenendo, in base al proprio statuto, in aziende che operano in settori strategici per lo sviluppo del Paese e in grado di generare impatto rilevante sull'economia italiana. Per favorire percorsi di consolidamento, espansione e internazionalizzazione, gli interventi di CDP Equity mirano ad intercettare i più rilevanti *mega-trend*: dalla transizione energetica alla *digital transformation*, dall'industria 4.0 al commercio internazionale. Restano al di fuori del perimetro gli investimenti in *holding* finanziarie di partecipazioni diversificate. Attualmente CDP Equity detiene partecipazioni dirette in 14 società di cui 4 sono società quotate.
- ***Investimenti Indiretti*** agendo come investitore *cornerstone* in fondi diretti e fondi di fondi gestiti dalle società di *asset management* di cui è azionista, garantendone la piena autonomia operativa e gestionale. CDP Equity agisce seguendo una rigorosa disciplina di investimento con un processo che prevede un'attenta attività di negoziazione e *due diligence* (con particolare attenzione agli aspetti ESG) e gestione dei fondi partecipati. Attualmente CDP Equity detiene partecipazioni in 5 SGR e ha investito in 7 fondi gestiti dalle medesime SGR

### 1.1.3 Leonardo S.p.A.

Con oltre 49.000 dipendenti, Leonardo S.p.A. (nel seguito anche LND) è una delle maggiori realtà industriali internazionali operanti nei settori Aerospazio, Difesa e Sicurezza. Un approccio sostenibile di business e una strategia finanziaria disciplinata sono i pilastri principali sui quali si basa la creazione di valore per tutti gli stakeholder. Nel settore Sicurezza e Digital Transformation opera la Divisione Cyber Security che, sfruttando le sinergie tra information technology, comunicazioni, automazione, sicurezza fisica e digitale, mette a disposizione dei propri clienti know how, processi e tecnologie avanzate. Tale Divisione realizza piattaforme applicative per l'erogazione di servizi digitali, supportando l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle Agende Digitali nazionali ed europee.



TIM - Uso Interno - Tutti i diritti riservati.

Si presenta sul mercato come un provider globale di sistemi, prodotti e soluzioni all'avanguardia in grado di rispondere alla crescente domanda di tecnologie avanzate nei settori della sicurezza, dell'informatica, della protezione di informazioni, infrastrutture e territorio, nonché nella gestione di infrastrutture strategiche. Con circa il 12% dei ricavi del 2020, Leonardo è terza in Europa e quarta nel mondo tra le maggiori aziende che investono in Ricerca e Sviluppo nel settore dell'Aerospazio, Difesa e Sicurezza. Il contributo di Leonardo alla spesa in Ricerca e Sviluppo totale del Paese è molto rilevante: considerando solo la parte di spesa allocata in Italia, Leonardo rappresenta il 16,8% della spesa in Ricerca e Sviluppo dei settori a tecnologia alta e medio-alta del Paese e il 10,9% del totale degli investimenti diretti in Ricerca e Sviluppo delle imprese manifatturiere italiane. I processi di innovazione sono supportati da 10 LABS a livello internazionale, di cui 6 in Italia. Vanta pluriennali esperienze maturate presso le principali Amministrazioni Pubbliche Centrali e Locali, risultando negli anni spesso aggiudicataria dei principali Contratti Quadro Consip nell'ambito Applicativo, Infrastrutture e Sicurezza finalizzati a indirizzare il processo di Digital Transformation, tra cui il Contratto per l'affidamento di servizi in ambito Sistemi Gestionali Integrati per le Pubbliche Amministrazioni – Lotto 1 (2017-2022). Nel settore Sicurezza opera la **Divisione Cyber Security** che, sfruttando le sinergie tra information technology, comunicazioni, automazione, sicurezza fisica e digitale, mette a disposizione dei propri clienti know how, processi e tecnologie avanzate. Tale Divisione realizza piattaforme applicative per l'erogazione di servizi digitali, supportando l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle Agende Digitali nazionali ed europee. In particolare, vengono offerte soluzioni innovative per l'erogazione di servizi digitali nei seguenti ambiti, svolgendo il ruolo di partner d'eccellenza nel processo di Digital Trasformation:




- ***Soluzioni di Cybersecurity:*** Grazie al nostro know-how nella protezione di paesi e di infrastrutture nazionali critiche, forniamo soluzioni e servizi che garantiscono il massimo livello di protezione e resilienza, incrementando la capacità di anticipare le minacce, controllare i rischi e gestire efficacemente gli attacchi cyber.
- ***Comunicazioni professionali***: Le nostre reti integrate e piattaforme di comunicazioni sicure sono in grado di soddisfare i più stringenti requisiti di affidabilità, anche in situazioni di emergenza, richiesti da agenzie di pubblica sicurezza, protezione civile e infrastrutture critiche.
- ***Sistemi di gestione e controllo***: Progettiamo e sviluppiamo piattaforme integrate di comando e controllo per la sicurezza urbana, la protezione delle infrastrutture critiche e dei grandi eventi, la gestione delle emergenze e il controllo del territorio.
- ***Sistemi di automazione***: Forniamo sistemi di automazione per la gestione dei bagagli negli aeroporti, basati su tecnologia all'avanguardia cross-belt, e sistemi di smistamento, movimentazione e tracciatura di lettere e pacchi per operatori postali e corrieri.



TIM - Uso Interno - Tutti i diritti riservati.

- ***Soluzioni per mercati***: Offriamo soluzioni innovative chiavi in mano, ritagliate sulle esigenze di sicurezza specifiche di ogni mercato, volte a migliorare la sicurezza dei cittadini e l'efficienza e la resilienza di organizzazioni pubbliche, private e delle infrastrutture critiche.

### 1.1.4 Sogei SpA

Sogei - Società Generale d'Informatica S.p.A. – è la società di Information Technology, partner tecnologico del Ministero dell'Economia e delle Finanze e interamente partecipata dallo stesso, che opera sulla base del modello organizzativo dell'in-house providing.

Nata nel 1976 come società a partecipazione pubblica, in esecuzione di una specifica previsione normativa, per la realizzazione dell'Anagrafe tributaria, Sogei è oggi la "piattaforma digitale" dell'Amministrazione Finanziaria, che offre soluzioni, competenze e asset, all'interno di un'infrastruttura strategica altamente affidabile.

Ulteriori previsioni normative hanno negli anni esteso negli anni la lista delle pubbliche amministrazioni e istituzioni Clienti, ampliando know-how e competenze e rendendo l'Azienda una risorsa unica del Paese, per efficienza, solidità, sicurezza e alta affidabilità, capace di tradurre le esigenze di innovazione dei propri Clienti in benefici per cittadini, imprese e istituzioni. "Semplifichiamo la vita di Noi cittadini" è il Purpose di Sogei ed è insito nella storia, nell'identità e nella cultura. È ciò che l'Azienda mette al servizio e che tiene conto delle esigenze e dei bisogni delle persone. Semplificare la fruibilità dei servizi e, quindi, la vita di tutti, supportando la digitalizzazione della PA per un'Italia più moderna e competitiva.
La Società ha 2.210 dipendenti (dati al 31 dicembre 2020) e una partecipazione di minoranza nella società Geoweb, società in controllo pubblico, costituita insieme al Consiglio Nazionale geometri e Geometri Laureati per offrire servizi IT ai professionisti.

## 1.2 Glossario

Salva diversa esplicita indicazione, ai termini seguenti, riportati in ordine alfabetico, viene attribuito, ai fini del presente documento, il significato di seguito indicato.

| TERMINE | DEFINIZIONE |
|---|---|
| AgID | Agenzia per l'Italia Digitale |
| Applicazione | Una qualsiasi realizzazione software (ad-hoc o prodotto di mercato) tesa a fornire un insieme di funzionalità alla PA. Solitamente una applicazione è composta da uno o più moduli software e da un database a cui l'applicazione fa riferimento |
| Costituendo ATI | Associazione Temporanea d'Impresa promotrice del progetto di fattibilità |
| Committente | Ministero per l'Innovazione Tecnologica e la Digitalizzazione |
| Contratto | L'atto che verrà stipulato tra la PA e la NewCo PSN, nel quale sono enunciate le regole giuridiche alle quali si dovrà conformare il Servizio |



TIM - Uso Interno - Tutti i diritti riservati.

| TERMINE | DEFINIZIONE |
|---|---|
| Centro Servizi | Il Centro Servizi della NewCo PSN rappresenta l'insieme di tutte le infrastrutture fisiche (Data Center), delle componenti hardware e software in essi ospitati e delle risorse destinate all'erogazione dei Servizi oggetto del presente Progetto di fattibilità |
| CSP | Cloud Services Provider, anche detti *Hyperscaler*, fornitori di servizi di cloud pubblico su scala mondiale |
| Fornitura | l'insieme dei prodotti software, hardware, dei servizi e di tutto ciò che è richiesto nel presente Progetto di Fattibilità |
| NewCO | Società di scopo |
| Servizi professionali | Gestione sistemistica, supporto specialistico ed evolutivo, servizi di sicurezza, servizio di assistenza |
| SLA | Service Level Agreement, ovvero "indicatori di prestazione chiave", e cioè quegli indicatori che permettono di misurare le prestazioni di una determinata attività o di un determinato processo |

## 1.3 Contesto tecnologico

I Sistemi Informatici delle PA sono costituiti da più sistemi di elaborazione dislocati presso Data Center per lo più ospitati all'interno delle strutture stesse delle PA, interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività).

Le PA hanno da tempo investito nelle architetture open coerentemente con le indicazioni tecnologiche del mercato e dell'Agenzia per l'Italia Digitale, ma la situazione attuale registra una presenza, per esempio, di variegati sistemi operativi quali Linux, Unix, Windows Server 2003, 2008, 2012.

Tale situazione inoltre non garantisce attualmente la continuità operativa dei servizi, né tantomeno l'architettura degli attuali Data Center delle PA è pensata per erogare i servizi di Business Continuity, operando quindi in alta affidabilità con modalità di allineamento active–active Geografico. Inoltre, la costituzione di molteplici data center locali ha generato:

- lock in tecnologico da parte dei Vendor;
- obsolescenza tecnologica per gli elevati investimenti richiesti per mantenere allo stato dell'arte l'infrastruttura;
- difficoltà a gestire la sicurezza delle informazioni non riuscendo a tenere il passo con il rapido evolversi delle minacce informatiche;
- difficoltà ad implementare processi standard di gestione dei servizi ad elevati standard qualitativo dovendo spesso ricorrere a personale esterno, specialmente per servizi critici H24;



TIM - Uso Interno - Tutti i diritti riservati.

- difficoltà a gestire rapidità nella messa in esercizio di nuovi servizi dovendo spesso aspettare l'esito di procedure negoziali per aggiornare o incrementare la capacità del Data Center.

Occorre quindi che le attuali architetture progrediscano dalla situazione attuale per evitare la presenza di alcun "single point of failure", garantendo quindi la ridondanza di tutti i sistemi e le apparecchiature che rivestono carattere di criticità per l'erogazione di un servizio continuo ad alta affidabilità.

Il contesto descritto è quello di riferimento alla data di stesura del presente Progetto di fattibilità. A valle della stipula del contratto, secondo le modalità e le tempistiche indicate al paragrafo 2.11***Servizio di Migrazione, Evoluzione e Professional Services***, ogni PA aderente all'iniziativa fornirà l'elenco aggiornato e dettagliato del perimetro IT e TLC coinvolto nell'affidamento dei servizi oggetto di gara.



TIM - Uso Interno - Tutti i diritti riservati.

## 1.4 Presentazione di Progetto

Questo paragrafo vuole dare una visione complessiva dell'intero progetto.

I principi che lo costituiscono sono dettagliati nei successivi e puntuali capitoli che ne descrivono servizi e caratteristiche.

La nostra Compagine è stata costituita per garantire l'aderenza nativa ai principi di disegno del PSN e per dare garanzie di solidità tecnica e finanziaria al progetto ed è composta da:



**Istituto Nazionale di Promozione**, abilitatore della politica industriale del paese attraverso investimenti in settori strategici quali le infrastrutture di rilevanza critica.

**Socio a garanzia** del controllo dello Stato e del supporto agli investimenti e al dialogo con la PA.



**Leader nel settore della sicurezza tecnologica** tra i primi 10 gruppi al mondo per expertise sui temi di digital security.

**Socio industriale con significativa expertise** in termini di security.



**Player di riferimento** per la fornitura di servizi informatici e di consulenza ICT alla Pubblica Amministrazione.

**Socio industriale** con expertise nel servire la PA.



**Uno dei più importanti gruppi Telco al mondo**, market leader in Italia nei servizi Cloud, Data Center e di connettività per la PA (11% quota di mercato).

**Partnership industriale con Google in ambito cloud**, per garantire trasferimento tecnologico e know how.

I principi che hanno ispirato il disegno del PSN sono:

- **Sovranità digitale e controllo statale**: garantire il controllo del PSN in capo allo Stato.
- **Sicurezza**: assicurare un presidio tecnologico e operativo in grado di garantire i più alti standard di sicurezza.
    - **Fisica** (e.g. disaster recovery, business continuity, controllo accessi, etc..);
    - **Informatica** (e.g. prevenzione e risposta attacchi cyber, data protection, identity access management, etc.).



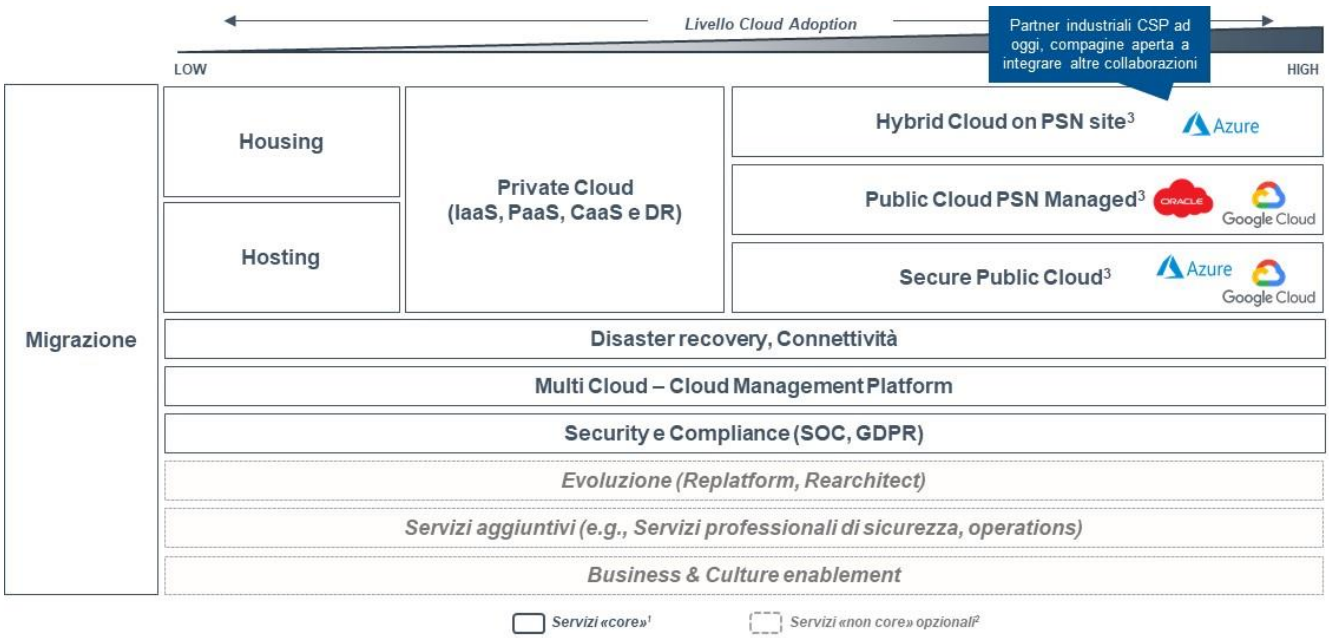
TIM - Uso Interno - Tutti i diritti riservati.

- **Innovazione**: pieno accesso alle migliori soluzioni tecnologiche per le infrastrutture data center, la connettività, le piattaforme e i servizi cloud, garantendo trasferimento tecnologico di esperienze e know how con i leader globali.
- **Conoscenza della PA**: dimestichezza con le dinamiche di fornitura di servizio, velocità nel rispondere alle necessità e referenze pregresse.

La proposta della Compagine è fondata su alcune assunzioni, di seguito elencate:

- **4 Data Center**, a partire da circa 800 mq. disponibili a T0 (comprensivi di connettività) fino a 2900 mq nello scenario di massima adesione.
- **Massima flessibilità** nell'offerta di servizi (housing, hosting, private cloud, hybrid cloud, public cloud).
- **Sovranità del dato**, elevati livelli di sicurezza (sarà allineato alla direttive ACN).
- **Società di scopo (NewCo PSN)**, operativa con circa 100 FTE a regime.
- **Adesioni** delle PA stimate non al 100% del perimetro.
- **Durata** della Convenzione per singola PA aderente di 10 anni.
- **Refresh tecnologico** all'anno 5.
- **Garanzia di evoluzioni tecnologiche** (nuovi servizi) e revisione dei prezzi secondo l'andamento del mercato.

L'offerta del PSN è costruita per essere la più ampia possibile per permettere a tutte le PA di scegliere i servizi più idonei alle loro necessità.





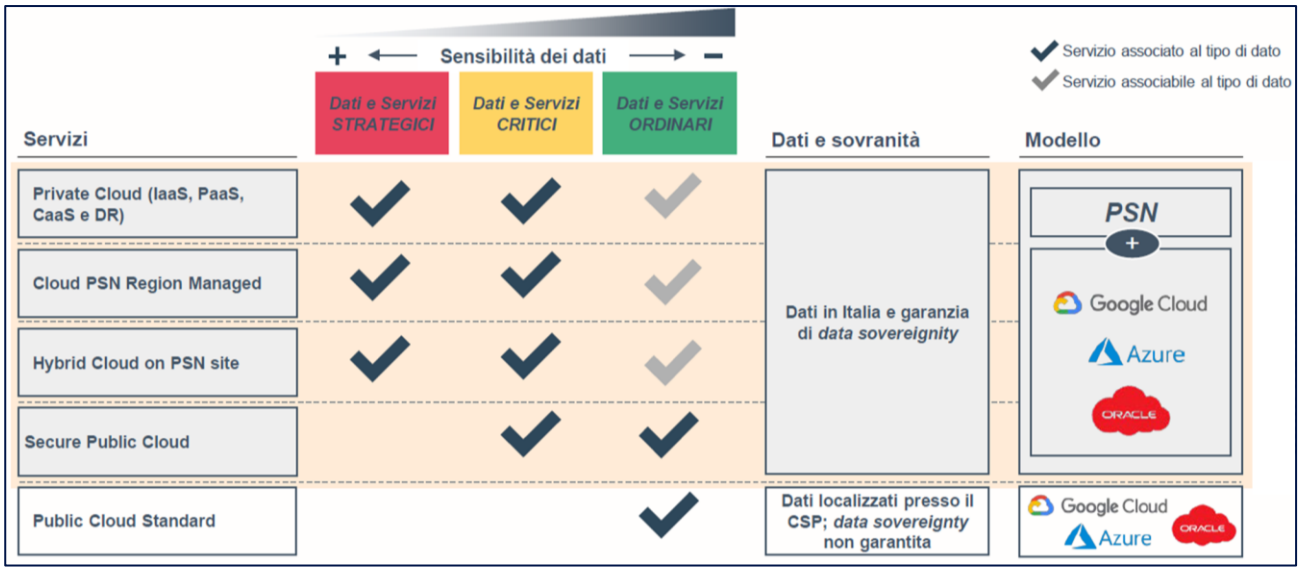

TIM - Uso Interno - Tutti i diritti riservati.

*Note: (1) Servizi per razionalizzazione, «messa in sicurezza» e adeguamento tecnologico e innovazione delle infrastrutture IT delle PA; (2) Servizi a disposizione delle PA, funzionali all'ulteriore evoluzione dei servizi (o a bisogni contingenti); (3) In grado di operare in modalità private, hybrid e public.*

Di seguito sono sintetizzati e schematizzati i servizi "core" e "no core" offerti alle PA.

| Servizi | | Descrizione (Servizi «core» / Servizi «non core» opzionali) |
|---|---|---|
| Migrazione | | • Migrazione end-to-end **chiavi in mano** sia **fisica** che **virtuale** (dall'analisi applicativa al test sui nuovi ambienti e messa in produzione) |
| Housing e Housing | | • Servizi di **gestione infrastrutturale** tradizionali. In caso di housing, il cliente utilizza lo spazio attrezzato di proprietà del provider in cui colloca i propri server, a differenza dell'hosting, in cui il cliente ha la possibilità di noleggiare i server di proprietà del provider |
| Private Cloud | IaaS dedicato | • Offerta di **infrastruttura virtualizzata** (capacità computazionale e storage) in modalità cloud, on demand e *as a service*, con possibilità di noleggiare server virtuali di proprietà del provider |
| Private Cloud | Iaas Shared | • Servizi **on demand private cloud infrastrutturale** (area Cloud dedicata per il cliente) |
| Private Cloud | CaaS e DR | • **CaaS (Container as a Service):** servizio cloud con possibilità di sviluppare applicazioni in ambienti «cloud native»; **DR (Disaster Recovery):** servizio back up dei contenuti informativi conservati in Cloud |
| Private Cloud | PaaS | • Messa a disposizione di **piattaforme** in grado di erogare **elementi applicativi e middleware** come servizio (database, big data, AI) |
| Soluzioni con CSP | Hybrid Cloud on PSN site | • **Servizi del CSP** (Cloud Service Provider) **hybrid** (combinazione di Cloud pubblico e privato mediante un'infrastruttura integrata) e **installati sull'infrastruttura locale** del PSN |
| Soluzioni con CSP | Public Cloud PSN Managed | • **Portfolio dei servizi CSP erogato da «Region» dedicata al PSN**, con separazione logico/fisica e operata e controllata da personale PSN |
| Soluzioni con CSP | Secure Public Cloud | • Servizi di **messa in sicurezza** di un sottoinsieme del **portafoglio di offerta relativo a un CSP** |
| *Servizi aggiuntivi* (Security Profess. Services incl. Security Compliance) | | • Servizi professionali per il **miglioramento della sicurezza delle infrastrutture** e delle **applicazioni della PA** |
| *Evoluzione* (Re-platform, Re-architect) | | • Servizi professionali evolutivi volti al **ridisegno delle applicazioni in ottica Cloud** |
| *Servizi aggiuntivi* (IT infr. Service Operations) | | • Servizi di **Managed Services** per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni |
| *Business & Culture enablement* | | • Servizi di **formazione / consulenza alle PA** per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità |

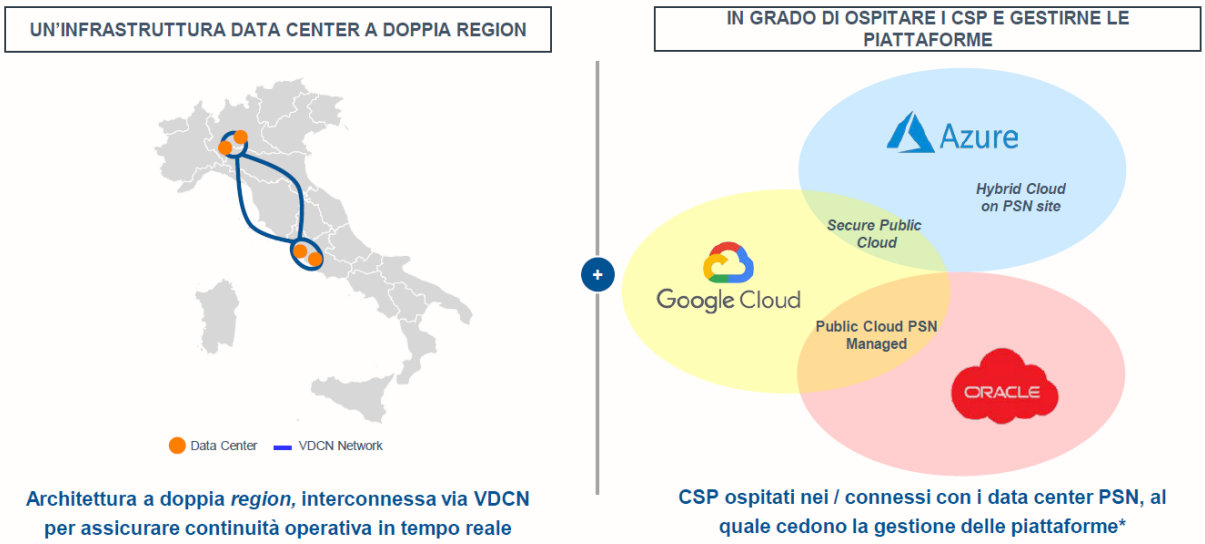
Attraverso il PSN ogni PA potrà scegliere le soluzioni cloud più adatte a garantire innovazione ma anche privacy, sicurezza, compliance, efficienza e sovranità del dato.




Il rapporto industriale con i Cloud Services Provider (CSP) è profondo: risiederanno nei data center del PSN e sono pronti a cedere al PSN la gestione delle loro piattaforme.



TIM - Uso Interno - Tutti i diritti riservati.




Questo rapporto industriale permetterà al PSN di erogare un set di servizi Cloud in collaborazione con i CSP.
Il PSN **offrirà soluzioni di sicurezza in linea con le normative, le best practice italiane, europee ed internazionali** secondo il modello descritto in figura. Per una descrizione più dettagliata si rimanda al § 3 Sicurezza.

| | | |
|---|---|---|
| FISICA | Presidio strutture | • **Videosorveglianza** integrata, **vigilanza** armata 24/7, **sensori** perimetrali, **standard ISO 27001**, … |
| | Controllo accessi Identità e permessi | • Restrizioni al personale autorizzato con **verifica multi-layer credenziali accesso** (one time password, parametri biometrici…) |
| | Protezione HW | • **Compartimentazione accessi** anche all'interno del DC, verifica movimentazione HW basata su seriali… |
| LOGICA | Endpoint & Data Protection | • Crittografia dei dischi, Software Antivirus e EDR, gestione dei dispositivi mobili, File Integrity Monitoring |
| | Identity, Access & Key Management | • Identity&Access Governance, Privileged Access Management, Authentication Management e MultiFactor Authentication. Gestione delle chiavi di cifratura e HSM |
| | Infrastructure & Network Security | • Segregazione degli ambienti, Accesso controllato, Hardening, Next Generation Firewall, Accesso Zero Trust, e-Mail&Web Security, Network Access Control. |
| ORGANIZZATIVA | Piano di Sicurezza | • Redazione, implementazione e manutenzione di un **piano di sicurezza** |
| | Conformità | • Processi di conformità **a normative di sicurezza italiane ed europee**, e a **standard e best practice** |
| | Organizzazione per la gestione della sicurezza cibernetica | • Definizione della costituency, erogazione di servizi di sicurezza da **SOC** e **CERT** specializzati |

*Nota: fonte dati sulla situazione attuale della PA da MID, su base censimento.*

Verrà predisposta un'unita organizzativa caratterizzata da specifici elementi di autonomia e indipendenza, al fine di garantire e assicurare la tutela delle infrastrutture e dei servizi considerati essenziali agli interessi e alla sicurezza nazionali.
La governance e la gestione sarà affidata a personale altamente competente in materia di Cyber Security. L'unità organizzativa di sicurezza ha l'obiettivo di garantire l'attuazione dei massimi protocolli di sicurezza attraverso:

- lo sviluppo del **Piano di sicurezza**



TIM - Uso Interno - Tutti i diritti riservati.

L'Organizzazione di Sicurezza predisporrà uno specifico e dettagliato Piano di Sicurezza redatto in conformità con i criteri di accreditamento AgID relativi ai PSN, che conterrà:

- una sintesi delle normative di riferimento applicabili;
- una generale ricognizione degli asset informatici;
- le criticità, anche solo potenziali;
- gli obiettivi di sviluppo, manutenzione e gestione, atti a garantire la corretta erogazione dei servizi;
- le risorse strumentali ed economiche necessarie.

- **Attività di controllo**

All'Organizzazione di Sicurezza saranno attribuiti compiti di controllo e supervisione in relazione alla corretta implementazione nei vari ambiti operativi.
Il Responsabile di tale organizzazione potrà essere individuato in accordo con le autorità istituzionali competenti e sarà dotato di specifici requisiti (es. NOS, cittadinanza italiana).

- **Operations**

Sul piano delle Operations, l'Organizzazione di Sicurezza, svilupperà, in particolare, le funzioni di **Security Operation Center (SOC)** e di **Computer Emergency Response Team (CERT)** e garantirà tutti i livelli di sicurezza previsti dalle normative vigenti, la presenza di un ambiente sicuro e protetto e la protezione dei dati personali trattati.

| | |
|---|---|
| End Point Security | Real Time Security Monitoring |
| Identity & Access Management | Training & Awareness |
| Key Management | Incident Response |
| Security Platform Management | Security Testing & Vulnerability Management |
| Security Policy management & Enforcement | Threat Intelligence & Infosharing |

*Attività operative*

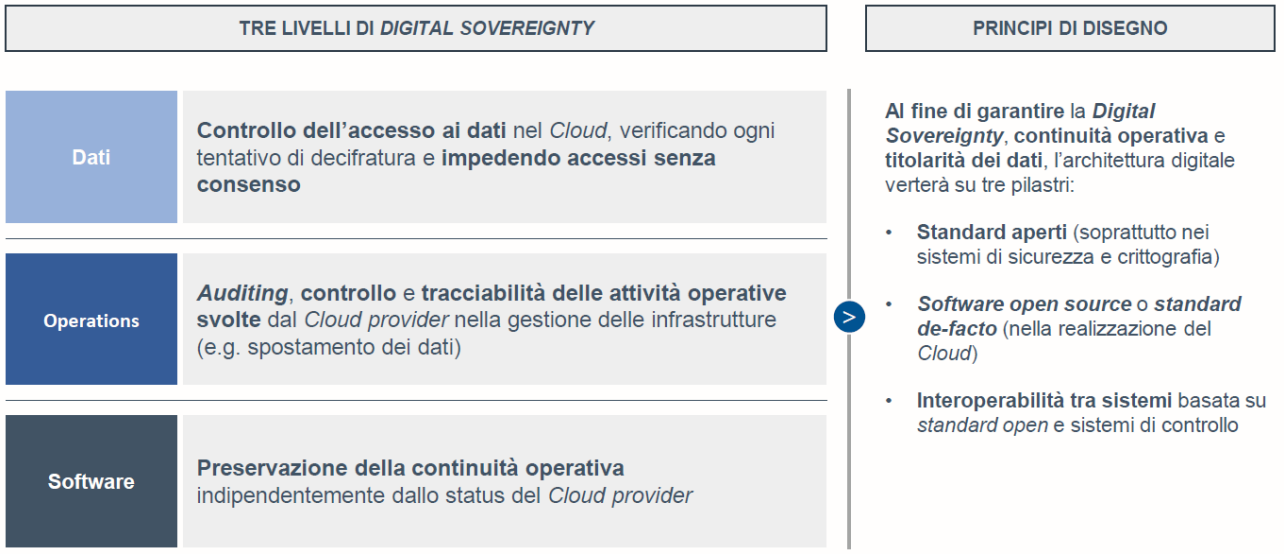
La proposta di questa compagine rappresenta **un'offerta di servizi gestiti ricca**, in grado di accompagnare la PA lungo tutto il journey del cloud, dalla migrazione all'assistenza.

| FASI PROGETTUALI | TRASFERIMENTO KNOW HOW |
|---|---|
| **Disegno e Implementazione** | ▪ **Assessment** delle infrastrutture IT, **progettazione** dell'infrastruttura, dell'architettura e **servizi di consulenza** per piani di migrazione e supporto alla trasformazione digitale **in collaborazione con la PA**<br>▪ **Gestione operativa eseguita con la PA e per la PA** garantendo trasferimento di know how verso i **dipendenti pubblici** che utilizzeranno i servizi del PSN |
| **Utilizzo giornaliero dei servizi** | ▪ Nella fase di execution, **graduale accompagnamento della PA** nel modello di gestione attività (monitoraggio, gestione infrastrutturale, ottimizzazione costi, …) **a regime**<br>▪ **Il PSN supporterà il personale della PA** nell'apprendimento necessario all'utilizzo di tool che consentano **la gestione dell'infrastruttura Cloud in autonomia** (e.g., piattaforme di self-provisioning) |



TIM - Uso Interno - Tutti i diritti riservati.

Al termine della concessione, alla PA sarà garantita la proprietà dei dati e la continuità operativa in base ai principi della Digital Sovereignty.




Si riportano di seguito i **punti di forza della proposta presentata** che sono supportati dalle soluzioni di seguito descritte:

1. **Public Cloud PSN Managed (Managed Region)**: **collocata** negli stessi **Data Center** delle soluzioni **Industry Standard**, controllata e gestita da **personale PSN italiano**, con rilasci degli **aggiornamenti SW controllati e certificati**.

2. **Secure Public Cloud**: le chiavi di **crittografia non risiedono** all'interno del **cloud CSP** ma sono **esterne**, sotto il totale **controllo del PSN**, duplicate per garantire **affidabilità**, **ridondanza** e **ottimizzazione** dei **tempi** di accesso. Nel caso di Secure Public Cloud con CSP Google la gestione è LAN to LAN (stesso Data Center).

3. **Hybrid Cloud on PSN Site**: **Architettura hybrid controllata e certificata**, controlli sulla "frontiers" di interconnessione con la componente Public, collocata negli stessi Data Center delle soluzioni Industry Standard.

4. **Sintesi delle proposte CSP**: **3 diverse possibili soluzioni**, tutte e tre contemporaneamente attive, **3 CSP complessivamente coinvolti con 2 CSP** a presidio di ogni **soluzione** (la soluzione di Oracle per la Region è funzionalmente sovrapponibile alla proposta Hybrid). Massima **indipendenza** dal **singolo CSP**, nessun servizio è erogato in modalità esclusiva.

5. **Caratteristiche societarie**: circa **100 persone assunte direttamente**, **management** scelto per **professionalità** e **garanzia** di **indipendenza** rispetto ai costi. Procedure di Sicurezza e



TIM - Uso Interno - Tutti i diritti riservati.

Compliance dedicate ed esclusive per la gestione del PSN. Disponibilità a **dotare** tutto il **personale** del **NOS** e la società del **NOSI**.

6. **Soci Industriali**: la forza della compagine, **Asset proprietari** (Data Center), **capacità** di fornire **connettività fissa** e **mobile** (5G), **Adozione** di **soluzioni Edge** per la prossimità, **garanzia** di un **player** attivo sulla **Sicurezza Nazionale**, le **migliori esperienze di migrazione** al **Cloud** della **PA**.

7. **Ruolo di CDP** come **investitore istituzionale** di garanzia che "ha **selezionato**" la **miglior formazione** possibile anche in termini di "**sovranità**" della proposta.

## 1.5 Oggetto della Fornitura

### 1.5.1 La NewCo

Il costituendo ATI al fine di mettere a disposizione delle Amministrazioni un servizio a loro dedicato, in grado di aiutarle e supportarle in tutte le fasi di vita di un contratto, **intende costituire,** a seguito dell'aggiudicazione della relativa gara, **una società di scopo** ("**NewCo**") opportunamente dimensionata. Tale nuova società sarà organizzata con Strutture Tecniche, Strutture Operative, di Sales & Marketing e figure di Staff.

Nel dettaglio le Strutture Tecniche si occuperanno degli ambiti relativi a:

- Network;
- Security;
- IT Infrastructure e Housing;

le Strutture Operative si occuperanno di:

- Management;
- Governance;
- Logistica;
- Project Management;
- Facilities DC;
- eProcurement.

Le funzioni di Sales & Marketing saranno impiegate nella promozione e nella commercializzazione dei servizi PSN oltre che nel Marketing dei servizi.
Le funzioni di staff ricomprendono ruoli quali:

- CFO;



TIM - Uso Interno - Tutti i diritti riservati.

- Audit;
- BD&S;
- Legal;
- Human Resource;
- Rapporti con Stakeholder;
- IT Staff.

La NewCo avrà ovviamente un proprio Amministratore Delegato ed un Presidente.

La NewCo PSN ha dimensionato la NewCo prevedendo un impiego di **oltre 80** persone per adempiere ai ruoli ed alle attività sopra indicati; ovviamente la NewCo si avvarrà anche di personale esterno in supporto al personale interno.

La NewCo PSN oltre al personale (interno ed esterno) si avvarrà del contributo dei soci industriali Leonardo, Sogei e TIM.

Nel prosieguo del presente Progetto di fattibilità si farà sempre riferimento alla NewCo come soggetto che avrà la responsabilità di erogare i servizi. In attesa di definire la ragione sociale della società di scopo, verrà denominata "**NewCo PSN**".

### 1.5.2 Tipologia di servizi erogati dalla NewCo PSN

La Fornitura prevede l'erogazione alle PA, secondo lo standard ISO 20001 per la gestione dei servizi IT in maniera continuativa e sistematica, di un Catalogo di Servizi, dedicati e con estremo focus su sicurezza, connettività ed affidabilità. I servizi offerti, oltre a quelli trasversali riportati di seguito, saranno suddivisi in "*Core*" e "*no Core*" (o Opzionali) e vengono individuati i **Service Elements** in relazione alle modalità di erogazione dei Servizi Infrastrutturali.

- Servizi di **Gestione della Sicurezza IT, a standard ISO 27001**
- Servizi di **Disaster recovery** e **Business Continuity, a standard ISO 22301l**
- Servizi di **Assistenza** ai fruitori dei servizi erogati
- **Console Unica** di gestione.

Con ✓ indichiamo i Service Elements **necessari** in relazione alla modalità prevista.
I servizi trasversali sono i seguenti:



TIM - Uso Interno - Tutti i diritti riservati.

| Servizi | | Industry Standard | | | | | | Hybrid Cloud on PSN Site | Secure Public Cloud | Public Cloud PSN-Managed |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Housing | Hosting | IaaS | CaaS | PaaS | BaaS | | | |
| **Facility** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Connectivity** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Operational Continuity** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Maintenance & Helpdesk** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **IT Infrastructure** | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Service & SLA Management** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Monitoring** | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Operational & Security Management** | **Physical** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Network** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Hardware** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Hypervisor** | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Operating System** | | | On-Demand | ✓ | ✓ | ✓ | Only for PaaS and CaaS Services | Only for PaaS and CaaS Services | Only for PaaS and CaaS Services |
| | **Middleware** | | | | | ✓ | ✓ | Only for PaaS Services | Only for PaaS Services | Only for PaaS Services |
| | **Runtimes** | | | | | ✓ | ✓ | Only for PaaS Services | Only for PaaS Services | Only for PaaS Services |
| | **Application** | | | | | | ✓ | | | |
| | **Data** | | | | | | ✓ | | | |



TIM - Uso Interno - Tutti i diritti riservati.

### 1.5.3 Servizi Core

Di seguito si riporta l'elenco dei servizi individuati come Core:

- Servizi **Infrastrutturali on-demand:**
  - **Industry Standard (Hosting, Housing, IaaS, PaaS, BaaS, CaaS);**
  - **Public Cloud PSN Managed;**
  - **Secure Public Cloud;**
  - **Hybrid Cloud on PSN Site;**
- Servizi di **Migrazione**

### 1.5.4 Servizi no Core

Di seguito si riporta l'elenco dei servizi individuati come Opzionali:

- **Servizi di Evoluzione (Re-Platform e Re-Architect)**
- **Professional Services**
- **Business & Culture Enabling**

## 1.6 Servizi erogati dai Soci

La tabella che segue elenca i servizi/attività erogati dai Soci con relativa descrizione di fornitura.

| Servizi/Attività erogati dai Soci al PSN | Descrizione della fornitura |
|---|---|
| **1. Spazi Attrezzati** | Canone relativo a:<br>•Affitto di 4 Data Center attrezzati e dedicati al PSN certificati Tier IV di cui 2 con disponibilità di sale Tier III, localizzati in doppia Region per garantire business continuity e soluzioni di Disaster recovery in logica High Availability per permettere un Backup real-time.<br>•Acquisto di cablaggi in componente attiva (e.g. configurazione VLAN, firewall, router) e in componente passiva (e.g. cavi, switch). |
| **2. Connettività** | •Connessione ad alta velocità per il collegamento dei Data Center (intra region e infra region).<br>•Servizio di protezione degli IP da cui le Amministrazioni erogheranno i propri servizi attestati sull'infrastruttura Industry Standard. Servizio progettato per «surgical mitigation», agendo sul traffico per singolo IP attaccato. |
| **3.Energia** | Fornitura di energia elettrica per l'infrastruttura IT del PSN. Il servizio viene erogato dai soci, i quali possono utilizzare accordi in essere con i propri fornitori a condizioni vantaggiose per il PSN. |



TIM - Uso Interno - Tutti i diritti riservati.

| Servizi/Attività erogati dai Soci al PSN | Descrizione della fornitura |
|---|---|
| **4.COPS - servizi di gestione cliente (Help Desk di primo livello)** | Servizio di Help Desk di primo livello dedicato ai clienti del PSN. Il servizio viene erogato da uno dei soci che, operando servizi di Help Desk di grandi dimensioni, può generare benefici per il PSN in termini di efficienza, qualità e scalabilità. |
| **5. Service Management - servizio di gestione del cliente** | Servizio di gestione delle interazioni con le PA composto da referenti dedicati per ogni amministrazione per attività di governance del servizio, reportistica e escalation delle richieste cliente. Il servizio viene gestito da un socio che già possiede una struttura consolidata di Service Management in ambito technology. |
| **6. Security Operations** | Servizio di Security Operations (inclusivo di attività di SOC) fornito dal socio con maggiore esperienza ed asset in ambito sicurezza in grado di generare benefici per il PSN in termini di efficienza, qualità e scalabilità. |
| **7. Sicurezza CERT** | Gestione di incidenti informatici sia in modalità proattiva (gestione delle vulnerabilità e delle minacce e prevenzione) sia in modalità reattiva (gestione tempestiva degli incidenti). Servizio erogato da un socio con infrastruttura CERT già predisposta e operativa. |
| **8. Servizi Professionali di Sicurezza** | Attività di Strategy & Compliance, assessment di sicurezza su infrastruttura e parco applicativo e supporto alle Operations per il mantenimento degli elevati standard di sicurezza. |
| **9. Secure Public Cloud** | Servizio di Key management, Template, Backup e di erogazione del servizio di Secure Public Cloud, progettato tramite accordo industriale tra soci e i CSP (Azure e GCP). |
| **10. Hybrid Cloud on PSN Site** | Gestione operativa del servizio e delle attività di sicurezza connesse all'Hybrid Cloud, progettato tramite accordo industriale tra soci e il CSP (Azure) |
| **11. Public Cloud a PSN Managed** | Gestione dell'infrastruttura dedicata e relativa manutenzione, analisi di sicurezza e attività di SOC, sviluppo degli «Shim layers» per il collegamento a servizi esterni. Servizio progettato con specifico accordo industriale tra soci e CSP (Oracle e GCP). |
| **12. Business & Culture Enablement** | Servizi di formazione / consulenza alle PA per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità. Erogato da un socio con elevata conoscenza dell'infrastruttura digitale della PA. |
| **13. Re-Architect** | Servizi professionali evolutivi volti alla riprogettazione dell'architettura delle applicazioni in ottica Cloud. Erogato dai soci con profonda conoscenza dell'ambiente cloud. |



TIM - Uso Interno - Tutti i diritti riservati.

| Servizi/Attività erogati dai Soci al PSN | Descrizione della fornitura |
|---|---|
| **14. Re-Platform** | Servizi professionali evolutivi volti alla riprogettazione delle piattaforme che gestiscono le applicazioni della PA in modo da abilitarne la trasformazione verso il Cloud. Erogato dai soci con profonda conoscenza dell'ambiente cloud. |
| **15. Servizio di migrazione** | Servizio di migrazione end-to-end chiavi in mano sia fisica (housing) che virtuale (dall'analisi degli applicativi al test sui nuovi ambienti e messa in produzione) dell'infrastruttura IT della PA verso l'infrastruttura PSN. |
| **16. IT Infrastructure - Controllo produzione (gestione sistemistica)** | Servizi di Managed Services per garantire il mantenimento di funzionalità e/o ottimizzazione degli ambienti su cui insistono le applicazioni. Erogato dai soci con ampia esperienza nella gestione sistemistica dei Data Center. |
| **17. IT Infrastructure - Service Operations** | Servizi specialistici on demand a supporto delle Operations per la gestione dell'infrastruttura e del parco applicativo cliente. Erogato dai soci con ampia esperienza nella gestione operativa dei Data Center. |
| **18. PaaS Industry** | Installazione e manutenzione degli HW e SW necessari per erogare il servizio. Erogato da soci con ampia esperienza in soluzioni AI, Big Data e IAM. |
| **19. Servizi di intra-migrazione** | Servizio end-to-end di migrazione da servizi industry standard verso servizi Cloud avanzati per abilitare la trasformazione cloud della PA. |

## 1.7 Le Partnership della Compagine

Il RTI ha in essere molteplici accordi di partnership tecnologiche. Relativamente alle partnership strategiche con i Cloud Services Provider (CSP), anche detti *Hyperscaler*, la situazione è riportata nei paragrafi successivi.

### 1.7.1 Google Cloud

**Partnership con Google**

A marzo 2020 TIM e Google Cloud hanno sottoscritto un importante accordo di collaborazione della durata di 5 anni, rinnovabile per ulteriori 5 anni.
L'impegno congiunto di Google e TIM ha previsto la realizzazione di due Region in Italia (per complessive sei Availability Zone) con rilascio progressivo ad iniziare dal primo trimestre 2022. TIM può comunque ospitare altri Cloud provider nei propri Data Center.
L'accordo ha riguardato i seguenti ambiti:

- Il Set-up delle Region GCP (Google Cloud Platform) in Italia;
- L'attività di go-to-market congiunto sulla primaria clientela italiana pubblica e privata;
- La definizione di soluzioni di Edge Cloud;
- L'utilizzo delle soluzioni GCP per l'IT interno di TIM;



TIM - Uso Interno - Tutti i diritti riservati.

- Potenziali upside addizionali.

Le condizioni previste dalla partnership per quanto riguarda le attività commerciali possono essere estese ad altre aree geografiche dove è presente il gruppo TIM, previo accordo tra le parti.
TIM e GCP stanno lavorando congiuntamente per la realizzazione della soluzione a supporto della Region Dedicata GCP per il mercato italiano con uno specifico focus per la realizzazione del Polo Strategico Nazionale che costituirà la prima esperienza in assoluto di questo tipo in Italia per l'intero mercato dei CSP.
Le parti stanno definendo il modello di accesso alle infrastrutture GCP secondo un modello isolato e che garantisca la sovranità delle applicazioni e dei dati. A fronte di questo modello, GCP permette al personale TIM di accedere a specifiche aree di lavoro dedicate alla Pubblica Amministrazione. TIM in questo contesto garantisce il personale adeguato alla copertura, a ricevere il software di GCP, gestirne la messa in produzione e a gestire l'hardware e le parti di ricambio in linea con i più elevati livelli di servizio richiesti dai servizi cloud.
L'accordo della Region Dedicata per il PSN segue quello della Region italiana GCP in termini temporali; TIM fornisce il personale e le soluzioni per gestire in autonomia le tecnologie GCP. Il progetto in questione costituirà un'aggiunta, specifica per il Polo Strategico Nazionale, all'accordo industriale descritto sopra.

**Google Cloud Platform (GCP) è una piattaforma di servizi Cloud** gestita, altamente scalabile, che consente l'esecuzione di carichi di lavoro in ambienti diversi dalle macchine virtuali (Compute Engine) ai container (Google Kubernetes Engine), fino a soluzioni serverless (CloudRun, AppEngine, Cloud Function).

GCP offre servizi IaaS, PaaS e SaaS su vasta scala, che spaziano dall'intelligenza artificiale al machine learning, dal datawarehousing a soluzioni di DevOps, dall'Api Management a soluzioni che facilitano scenari ibridi. La connessione con gli ambienti on-premise, disponibile in diverse modalità (Cloud VPN, Dedicated e Partner Interconnect, Peering) è assicurata da una dorsale di rete proprietaria in fibra ottica, in continua espansione, ad elevate prestazioni, che collega i vari data center distribuiti su scala globale, organizzati in zone di disponibilità e Region. Sono di prossima apertura le due Region italiane a Milano e Torino. Google Cloud Platform può contare su oltre 100 punti di presenza in 15 regioni globali. Con il Virtual Private Cloud (VPC) è possibile connettere le proprie risorse GCP o isolarle l'una dall'altra. Attraverso Cloud Delivery Network (CDN) il contenuto viene distribuito attraverso punti di presenza a livello edge e il servizio di Cloud Load Balancing può bilanciare il traffico HTTP(S), TCP/SSL e UDP. La migrazione in tempo reale di macchine virtuali e una varietà di backup ridondanti assicurano un'archiviazione sempre disponibile. Google Cloud dispone inoltre di un'articolata piattaforma per la gestione dei dati, dalla creazione, alla trasformazione all'analisi.

Google ha da tempo iniziato lo sviluppo di servizi per indirizzare le richieste di sovranità digitale (relative alle tre dimensioni dei dati, delle operazioni e del software). In questo ambito sono quattro le soluzioni offerte in cui il controllo dei dati e delle operazioni viene spostato progressivamente dal Cloud Service Provider ad un partner qualificato o all'amministrazione stessa:

- Public Cloud;
- Secure Public Cloud;



TIM - Uso Interno - Tutti i diritti riservati.

- Partner Managed Cloud;
- GPC.

I servizi di Google Cloud assicurano che il dato sia crittato sia at rest che in transit e, tramite il Confidential Computing, anche in memoria.

L'offerta Public Cloud di Google, già nativamente dotata del servizio di Key Management con gestione delle chiavi da parte di Google stessa o del cliente anche in moduli HSM, è stata arricchita con le funzionalità di External Key Manager (EKM), servizio che consente di conservare le chiavi crittografiche affidandole ad un operatore esterno a Google, realizzando così un Secure Public Cloud. A questo si aggiunge la funzionalità di Key Access Justification che consente l'auditing degli accessi alle chiavi con la possibilità di definire alert in caso di accesso non giustificato.

La soluzione Trusted Partner Cloud prevede la gestione da parte di un partner qualificato di una istanza della Google Cloud Platform, che gira in ambienti sotto il controllo del partner stesso, siano essi una porzione di un data center Google acceduto solo dal partner o in uno spazio dedicato di proprietà del partner. L'accesso a tali ambienti è precluso ai dipendenti Google, se non preventivamente autorizzati dal partner. Il partner è proprietario del Certificate of Authority, dei sistemi di identità, dell'infrastruttura e ha in custodia fisica l'intero hardware. Tutti i dati in transit e at rest sono criptati con chiavi gestite ed in possesso del partner che ha diversi livelli di controllo e della sicurezza: sicurezza applicativa, sicurezza del trasporto, controlli crittografici, sicurezza delle macchine, sicurezza fisica, rete logica e fisica. Google mantiene solamente la gestione dell'hardware e del software, assicurando i necessari aggiornamenti.

Per una gestione completamente disconnessa Google propone la soluzione Google Private Cloud, che consente, in un ambiente multi-tenant di proprietà del cliente o di un partner o in co-location, l'operatività della Google Cloud Platform su hardware certificato. Un cloud privato che offre le funzionalità e le capacità avanzate di Anthos, il servizio per la gestione centralizzata e multi cloud di ambienti containerizzati, combinate con un insieme di servizi della piattaforma e di terze parti forniti in una soluzione chiavi in mano che include l'infrastruttura (l'elaborazione, lo storage e il networking). Questa soluzione, pre-certificata e preconfigurata, offre al contempo livelli di servizio più elevati e garantiti, nonché la flessibilità di un modello autogestito o gestito da partner.

### 1.7.2 Microsoft Azure

**Partnership con Microsoft**

A maggio 2021 Leonardo e Microsoft hanno sottoscritto un Memorandum of Understanding volto a dare il via ad una collaborazione industriale che ha come finalità anche la realizzazione di progetti per la trasformazione digitale della Pubblica Amministrazione Italiana e per le infrastrutture critiche nazionali, focalizzandosi sulla protezione dei dati e l'impiego di tecnologie e soluzioni cloud avanzate, come quelle inserite nella proposta per il futuro Polo Strategico Nazionale (PSN).
Nell'accordo, Leonardo si candida al ruolo di System Integrator e responsabile della Cyber Security per la trasformazione digitale e il consolidamento dei data center della Pubblica Amministrazione, mentre Microsoft mette a disposizione tecnologie e servizi avanzati di produttività, sicurezza, cloud e automazione dei processi, per consentire l'accelerazione digitale della pubblica amministrazione e delle aziende Italiane.



TIM - Uso Interno - Tutti i diritti riservati.

In base a questo MoU, il personale di ingegneria di Leonardo e Microsoft ha collaborato in modo esclusivo alla definizione e alla progettazione delle migliori soluzioni per erogare servizi per il cloud cifrato (Secure Public Cloud) e per l'ibrido su licenza (Hybrid Cloud on PSN Site) all'interno del PSN. Questa collaborazione, facendo leva sulla possibilità di conoscere in anteprima le evoluzioni dei prodotti Microsoft, consente di inserire soluzioni più sicure e rende più ampia l'offerta prevista dal PSN.
In particolare, la conoscenza delle evoluzioni future delle soluzioni di confidential computing del cloud Azure ha permesso di inserire nella proposta del 29 settembre u.s. l'applicazione di scelte tecnologiche volte a migliorare la sicurezza complessiva del cloud cifrato garantendo così la piena sicurezza dei dati in uso.
Nelle soluzioni ibride su licenza, inoltre, gli approfondimenti fatti dai rispettivi team di ingegneria hanno consentito di prendere delle decisioni architetturali volte non a massimizzare le soluzioni attualmente in commercio come Azure Stack Hub, ma a disegnare scenari più in linea con le soluzioni strategiche che daranno la massima applicazione nel prossimo futuro essendo basate su Azure HCI e Azure Arc.
La progettazione congiunta ha permesso di creare un sistema di governance del cloud cifrato che innalza la sicurezza complessiva, limitando le azioni possibili da parte della PA pur preservandone la flessibilità operativa, con un approccio secure by policy. Questa tipologia di governance consente di ridurre il personale del PSN dedicato al controllo della postura di sicurezza delle singole PA.
Infine, la partnership Leonardo – Microsoft, laddove applicata al PSN Cloud, consentirebbe di influenzare le roadmap di prodotto e assicurare la disponibilità delle nuove tecnologie richieste, temporalmente allineate quanto più possibile con le esigenze del mercato italiano.

Fondata nel 1975, Microsoft è tra le più grandi aziende di tecnologia al mondo ed è il più grande fornitore di hyperscale cloud aziendali al mondo. La sua offerta copre tutti e tre i livelli del cloud, IaaS, PaaS, SaaS con specifiche soluzioni, tra i leader di mercato e tecnologicamente molto avanzate, per il mondo ibrido.

La vasta gamma di servizi cloud di Microsoft è incentrata sulla sua tecnologia Azure per IaaS e PaaS. Oltre a questi elementi fondamentali, Microsoft ha esteso la gamma di prodotti Azure ad intelligenza artificiale, machine learning, IoT, sicurezza, database, gestione dei dati e altro ancora.

Microsoft Azure è costituito da oltre 60 Azure Region collegate dalla Microsoft Global Network. È una presenza capillare, guidata dalla intenzione di avvicinare le applicazioni agli utenti in tutto il mondo, mantenendo la residenza dei dati e garantendo scalabilità, conformità, sicurezza e resilienza.

Ogni Azure Region è costituita da un set di data center distribuiti entro un perimetro definito dalla latenza e connessi tramite una rete regionale dedicata a bassa latenza. Ognuno di questi set di DC forma una Availability Zone (zona di disponibilità), ovvero una località separata fisicamente all'interno della Region e totalmente indipendente. Le Availability Zone consentono di eseguire applicazioni mission-critical in *High Availability* dove si possono utilizzare repliche database e applicative sincrone a bassa latenza distribuite su un'area metropolitana. Per garantire resilienza ad un disastro grave che possa impattare tutte le Availiability Zone di un'intera Region, si può realizzare una soluzione di DR in una Region Azure secondaria nella stessa area geografica.



TIM - Uso Interno - Tutti i diritti riservati.

La Microsoft global network impiega oltre 130.000 miglia di fibra ottica e di sistemi di cavi sottomarini ed offre oltre 160 punti di presenza (edge locations) nel mondo. Il traffico IP rimane interamente all'interno della rete globale e non entra mai nella Internet pubblica. I clienti possono collegarsi alla global network con connettività dedicata Express Route fino a 100Gbps o in alternativa, in VPN.

Azure è un cloud hyperscale di successo, adottato da più del 95% delle aziende Fortune 500 in tutti i settori industriali.

Per i governi e il settore pubblico di tutto il mondo, Microsoft offre Azure, una piattaforma di servizi cloud multi-tenant pubblica e le tecnologie per realizzare una soluzione ibrida, che puoi usare per distribuire varie soluzioni in base al livello di controllo, di gestione e di rispetto di normative sulla residenza del dato. Una piattaforma di servizi cloud multi-tenant implica che più applicazioni e dati dei clienti siano archiviati sullo stesso hardware fisico.
Azure usa l'isolamento logico per separare le applicazioni e i dati di ogni cliente, offre meccanismi di crittografia e la possibilità di eseguire servizi su infrastrutture di ultima generazione che consentono di crittografare dati e programmi con chiavi possedute solo dal cliente finale (confidential computing). Questo approccio offre la scalabilità e i vantaggi economici dei servizi cloud multi-tenant, aiutando rigorosamente a impedire ad altri clienti di accedere ai tuoi dati o alle tue applicazioni.

Le tecnologie ibride di Microsoft estendono queste funzionalità e possibilità anche nelle infrastrutture on-premise. Utilizzando le funzionalità del cloud pubblico di Azure, in congiunzione con le sue soluzioni ibride, è possibile beneficiare della rapida crescita delle funzionalità, della resilienza e del funzionamento conveniente del cloud hyperscale, pur ottenendo i livelli di isolamento, sicurezza e affidabilità necessari per gestire i carichi di lavoro in un ampio spettro di classificazioni di dati.
Utilizzando le tecnologie di protezione dei dati di Azure e le funzionalità perimetrali intelligenti del portafoglio di prodotti ibridi, è possibile elaborare dati riservati in un'infrastruttura isolata e sicura all'interno del cloud pubblico multi-tenant o dati riservati in locale e all'Edge, con la piena operatività e controllo.

Microsoft Azure è particolarmente attenta in merito alla residenza dei dati e ai criteri di trasferimento. Microsoft Azure consente di specificare l'area di distribuzione dei servizi utilizzati e per questi servizi, Microsoft non memorizzerà i dati al di fuori dell'area geografica specificata.
E' possibile usare opzioni di crittografia dei dati complete e affidabili per proteggere i dati in Azure e controllare chi può accedervi.
Microsoft possiede oltre 90 certificazioni e investe ogni anno un miliardo di dollari in Cybersecurity per proteggere a ogni livello i servizi Cloud. La nuova Region Data Center italiana aiuterà ulteriormente le aziende ad adempiere al regolamento generale sulla protezione dei dati dell'Unione Europea (**GDPR**) e permetterà alle aziende di far risiedere i dati in territorio italiano.

### 1.7.3 Oracle Cloud

**Partnership con Oracle**
TIM, Oracle e Noovle (gruppo TIM) hanno firmato a luglio 2021 un Memorandum of Understanding (MoU) che definisce una partnership industriale fondata sui seguenti punti:



TIM - Uso Interno - Tutti i diritti riservati.

- utilizzo delle Soluzioni Oracle Cloud per gli ambienti della pubblica amministrazione e in particolare per il Polo Strategico Nazionale;
- ospitare una Region Italiana di Oracle nei Data Center di TIM;
- abilitazione di Noovle come Cloud Service Provider di Oracle.

Attraverso questo agreement TIM completa il piano di servizio Multi Cloud anche a livello di nodo di connettività e aggiunge ai precedenti accordi un tassello fondamentale per fornire ai clienti differenti opzioni di uso del cloud pubblico.
L'accordo con Oracle mira alla creazione di Soluzioni Cloud di tipo data-driven e abilita TIM-Noovle ad erogare servizi in ambito Cloud di Oracle includendo specificamente servizi basati su appliance ingegnerizzate (Exadata), il Cloud@Customer e la Region Dedicata.

**Oracle Cloud Infrastructure (OCI) è una piattaforma ampia e profonda di servizi cloud pubblici** che consente ai clienti di creare ed eseguire un'ampia gamma di applicazioni in un ambiente scalabile, sicuro, ad alta disponibilità e ad alte prestazioni.

Oracle Cloud Infrastructure combina l'elasticità del cloud pubblico con il controllo granulare, la sicurezza e la prevedibilità prestazionale di un'infrastruttura locale per offrire servizi di tipo enterprise (ad alte prestazioni, alta disponibilità) con costi contenuti.
Oracle Cloud Infrastructure offre servizi di infrastruttura (IaaS), di piattaforma (PaaS) e di servizi applicativi (SaaS) attraverso un insieme di "Region" distribuite nel mondo ed in continua espansione.

Le Region sono organizzate in uno o più Availability Domain (AD): Data Center vicini tra loro (area metropolitana), collegati da un backbone ad alta velocità, ma indipendenti.

All'interno di un Availability Domain le risorse fisiche (ad esempio i server) sono organizzate in tre Fault Domain (FD) distinti, per garantire adeguata protezione da hardware e power faults.

Molti servizi Cloud prevedono la replica automatica dei dati su storage server collocati in Fault Domain distinti, in modo da assicurare adeguata protezione dei dati e il cliente può scegliere la collocazione delle VM in Availability Domain e Fault Domain distinti.
Per soddisfare requisiti stringenti in termini di sicurezza, privacy, residenza e sovranità del dato, Oracle, in aggiunta alle regioni di tipo Public, offre il suo portfolio completo di servizi IaaS, PaaS e SaaS all'interno dei data center Private con la soluzione di Oracle Dedicated Region Cloud @Customer (DRCC). Ogni DRCC è composta da un Availability Domain e tre Fault domains.
Le Oracle Dedicated Region Cloud @Customer rappresentano un'area autonoma e disconnessa dalle Public Regions in cui tutti i dati, inclusi operations e metadati, rimangono locali nel data center.

Per la componente Oracle Database è possibile utilizzare i servizi nativi OCI Database Cloud Service che offrono la possibilità di istanziare ed usufruire di un database Oracle gestito in cloud con diverse opzioni possibili per meglio rispondere alle esigenze ed aspettative del cliente.

Tra le caratteristiche native principali dei servizi Oracle Database Cloud troviamo:



TIM - Uso Interno - Tutti i diritti riservati.

- Automazione per il provisioning di istanze di servizio Oracle Database tramite console, API, SDK, CLI;
- Supporto e certificazione per ambienti in configurazione cluster (attivo-attivo in lettura e scrittura) con Real Application Cluster;
- Supporto a deploy del servizio in ambiente virtualizzato, bare metal ed Exadata per garantire stessi livelli di scalabilità, performance ad affidabilità di quelli attualmente ottenuti on-premise;
- Automazioni native per backup, restore, patching, upgrade, cloning, scaling per una fornitura “DB as a Service” out-of-the-box;
- Gestione nativa dei PDB (Pluggable Database);
- Automazioni per Disaster Recovery tramite utilizzo di Data Guard con database primario e di standby su Region diverse;
- Monitoring integrato per le istanze Database;
- Piena compatibilità applicativa con le tecnologie Oracle Database utilizzate on-premise per una migrazione senza rischi;
- Cifratura di tutti i dati con controllo delle chiavi di cifratura;
- Utilizzo del modello pay-per-use e possibilità di utilizzo delle licenze Oracle in possesso tramite opzione BYOL (Bring Your Own License);
- Disponibilità della versione cloud Autonomous Database per un servizio completamente gestito (patching, backup, scaling etc..) e ottimizzato per carichi di lavoro di tipo Transazionale o Datawarehouse.

Oracle ha collaborato con enti di valutazione esterni e revisori indipendenti per soddisfare un'ampia serie di standard di conformità internazionali e specifici per l'implementazione di servizi Cloud, come ISO 27001, SOC1, SOC2, PCI DSS, HIPAA / HITECH e FedRAMP.
Oracle Cloud è inoltre un CSP (Cloud Service Provider) qualificato da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018.

Oracle Cloud Infrastructure è stato il primo cloud provider ad implementare una virtualizzazione di rete completamente isolata (definita "off-box" isolated network virtualization), che mantiene la virtualizzazione di rete e I/O isolata dall'hypervisor e quindi dalle Virtual Machine. Di conseguenza, i clienti possono eseguire in self-service il provisioning delle proprie risorse host (virtual machine o bare metal dedicati) garantendo il completo isolamento delle risorse e senza risentire del workload e del traffico generato dalle risorse assegnate ad altri clienti.

## 1.8 Certificazioni del Personale

Le singole aziende del costituendo RTI nell’ambito degli accordi di partnership, sopra citati, al fine di governare e gestire al meglio le tecnologie dei CSP, hanno avviato programmi di certificazioni del proprio personale. Tale programma proseguirà nel corso del 2022 ed al momento consente alla compagine di poter disporre di:



TIM - Uso Interno - Tutti i diritti riservati.

- > 1.250 certificazioni personali Google;
- > 300 certificazioni personali Microsoft;
- > 100 certificazioni personali Oracle.

L'eccellenza dei tre partner tecnologici si basa su personale altamente qualificato non solo per le soluzioni Hyperscaler, ma anche per le principali tecnologie leader di mercato che compongono tutta l'architettura necessaria a rendere fruibili e sicure le infrastrutture cloud. Si riportano, di seguito, le ulteriori principali certificazioni di cui si è in possesso a livello di architetture cloud:

- > 400 certificazioni personali VMware;
- > 50 certificazioni personali Red Hat;

e per le componenti di networking e sicurezza perimetrale:

- > 2.000 certificazioni personali Cisco;
- > 100 certificazioni personali Fortinet;
- > 80 certificazioni personali Palo Alto;
- > 85 certificazioni personali Juniper.



TIM - Uso Interno - Tutti i diritti riservati.

# 2 Servizi Offerti e Modalità di Erogazione

La PA potrà selezionare dal Catalogo un'ampia offerta di Servizi, con una proposta sempre allo stato dell'arte, aggiornata secondo le più avanzate tendenze del mercato e allineata alle innovazioni introdotte dagli *Hyperscaler*. L'erogazione dei Servizi richiesti sarà regolata tramite apposito contratto; la PA condividerà l'elenco aggiornato delle proprie dotazioni tecnologiche, e la NewCo PSN proporrà il servizio a catalogo che meglio copre l'esigenza della PA. Alla stipula del Contratto, sarà possibile procedere con le attività di Migrazione, propedeutiche alla fruizione del Servizio. **Il Contratto tra le PA e la NewCo PSN non sono oggetto del presente Progetto di fattibilità.**
I servizi offerti sono disponibili nelle seguenti modalità;

- Housing dedicato
- Hosting dedicato - con opzione su Rack dedicati e condivisi
- IaaS:
  - Private
  - Shared
- PaaS (DBaaS, PaaS IAM, Big Data, Artificial Intelligence)
- BaaS
- DraaS
- CaaS
- Security
- Public Cloud PSN Managed
- Secure Public Cloud
- Hybrid Cloud on PSN Site
- Multi Cloud
- Servizi di Migrazione, Evoluzione e Professional Services
- Business and Culture Enablement

L'infrastruttura sarà ospitata all'interno di **4 Data Center,** allestiti in **doppia Region (2 DC + 2 DC)** dotati di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire i massimi standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti.

## 2.1 Housing

Il **Servizio Infrastrutturale in modalità Housing Dedicato** consiste nella messa a disposizione, da parte della NewCo PSN, di aree **esclusive** all'interno dei Data Center, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti descritti nel ***capitolo 3 –***



TIM - Uso Interno - Tutti i diritti riservati.

***Sicurezza*** *e* ***capitolo 4 - Infrastruttura IT e Network*** , atte ad ospitare le infrastrutture IT e TLC di proprietà delle PA, nonché di eventuali variazioni in corso d'opera.

## 2.2 Hosting

Il **Servizio Infrastrutturale in modalità Hosting Dedicato** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **fisica e dedicata**, in grado di ospitare tutte le applicazioni in carico alla PA all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica descritti nel ***capitolo 3 – Sicurezza e capitolo 4 Infrastruttura IT e Network.***

Le modalità di erogazione del servizio sono due:

- Hosting dedicato su rack condivisi: le PA avranno accesso a infrastruttura dedicata all'interno di porzioni di rack, che saranno condivisi con altre PA.
- Hosting dedicato su rack privati: le PA avranno accesso a infrastruttura dedicata all'interno rack esclusivi / segregati.

La NewCo PSN sarà responsabile di tutti gli aspetti di gestione e manutenzione dell'infrastruttura hardware su cui è costruito il servizio.

## 2.3 IaaS

I servizi di tipo Infrastructure as a Service (IaaS) prevedono l'utilizzo, da parte dell'Amministrazione, di risorse infrastrutturali virtuali erogate in remoto. Infrastructure as a Service (IaaS) è uno dei tre modelli fondamentali di servizio di cloud computing. Come tutti i servizi di questo tipo, fornisce l'accesso a una risorsa informatica appartenente a un ambiente virtualizzato tramite una connessione Internet. La risorsa informatica fornita è specificamente un hardware virtualizzato, in altri termini, un'infrastruttura di elaborazione. La definizione include offerte come lo spazio virtuale su server, connessioni di rete, larghezza di banda, indirizzi IP e bilanciatori di carico.




### 2.3.1 IaaS Private

Il **Servizio Infrastrutturale in modalità IaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **virtualizzata e dedicata**, in grado di ospitare tutte le applicazioni in carico alla PA all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica descritti nel §. 3 ***Sicurezza*** e nel §. 4 Infrastruttura IT e Network.

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante e mettere a disposizione gli strumenti e le console per la gestione in autonomia degli ambienti fisici e virtuali contrattualizzati.



TIM - Uso Interno - Tutti i diritti riservati.

### 2.3.2 IaaS Shared

Il **Servizio Infrastrutturale in modalità IaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **virtualizzata e condivisa**, in grado di ospitare tutte le applicazioni in carico alla PA all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica descritti nel §. 3 ***Sicurezza*** e §. 4 Infrastruttura IT e Network**.**

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

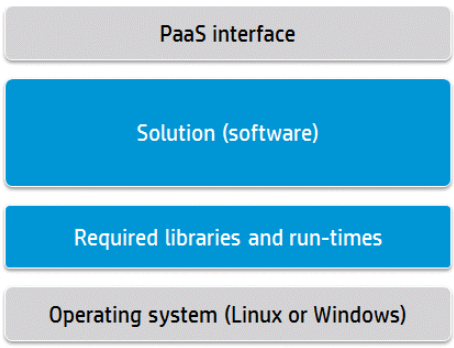
## 2.4 PaaS Industry

Il **Servizio PaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad esempio i Data Base, astraendo dall'infrastruttura sottostante.

La NewCo PSN, in qualità di provider, si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

L'offerta dei servizi PaaS prevede un approccio strutturato in cui ogni componente della soluzione PaaS, come il sistema operativo, solution stack ed altri software necessari, è strettamente controllato in termini di utilizzo e configurazione e gestito dal PSN. In questo caso le soluzioni vengono "create" al momento della necessità. Una rappresentazione di questa strutturazione vede quattro livelli di componenti:

- sistema operativo;
- run-time e librerie necessarie;
- soluzione caratterizzante – tipicamente un database, middleware, web server, ecc.;
- un'interfaccia programmatica con cui controllare gli aspetti operazionali della soluzione.




### 2.4.1 DBaaS

Il Database-as-a-Service è un servizio che consente agli utenti di configurare, gestire e ridimensionare database utilizzando un insieme comune di astrazioni secondo un modello unificato, senza dover conoscere o preoccuparsi delle esatte implementazioni per lo specifico database. Viene demandato al provider tutto quanto relativo all'esercizio e alla gestione dell'infrastruttura sottostante, comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche, mentre gli utenti possono così focalizzarsi sulle funzionalità applicative ed estrarre valore dai dati.

Tramite la console di gestione del servizio vengono messe a disposizione del cliente in particolare le funzionalità di:



TIM - Uso Interno - Tutti i diritti riservati.

- creazione (o cancellazione) di un database;
- modifica delle principali caratteristiche infrastrutturali dell'istanza DB e ridimensionamento ove non automatico;
- configurazione di alcuni parametri del database;
- attivazione di funzionalità aggiuntive, come ad esempio la replica dei dati su istanze passive (ove applicabile);
- attivazione di funzionalità di backup od esportazione dei dati (ove applicabile).

Altre funzionalità avanzate di configurazione delle specifiche istanze database sono demandate alle relative interfacce di amministrazione native.

Il catalogo del servizio comprende:

- **Database relazionali** (**Oracle DB Enterprise e Standard, MySQL, PostgreSQL, Maria DB, ...**) che supportano il modello dati relazionale e lo standard SQL di interrogazione. Sono quindi adatti a spostare carichi di lavoro di DB SQL preesistenti a casa del cliente su ambienti moderni e sicuri, in grado di garantire l'elevata affidabilità e le possibilità di crescita offerte dal Cloud.
- **Database NoSQL** (**MongoDB**, ...) ottimizzati per trattare dati non strutturati, con volumi elevati o con caricamento di grandi quantità di informazioni in modelli dati flessibili e con bassa latenza.

### 2.4.2 PaaS IAM

In aggiunta ai servizi di Identity and Access Management descritti al § 3.8.2che garantiscono i diritti di accesso alle componenti tecniche in ambito PSN (IaaS, PaaS, console unica di gestione, ecc.), viene reso disponibile dalla NewCo PSN un servizio di Identity Management applicativo che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano dentro il PSN.

Tale servizio ha lo scopo di integrare in modo facile e nativo le differenti esigenze di autenticazione e autorizzazione ad oggi previste all'interno del Codice dell'Amministrazione Digitale (CAD) ed in accordo con le normative vigenti in materia di trattamento dati riportate nel General Data Protection Regulation (GDPR).

Il servizio mette a disposizione le seguenti funzionalità:

- credenziali uniche di accesso alle applicazioni in perimetro e presidio efficace dei punti di accesso;
- implementazione di policy di cambio password, autenticazione a due fattori o semplicemente auditing e monitoring dei log di accesso;
- profilazione e segregazione delle informazioni in funzione dei propri privilegi: l'approccio di base si è concentra sulla creazione del "need-to-know". Le informazioni sensibili sono rese



TIM - Uso Interno - Tutti i diritti riservati.

disponibili solo a quelle persone dotate di adeguate autorizzazioni e di un "need-to-know" di tali informazioni per l'esercizio delle loro funzioni;

- controllo della diffusione delle informazioni: c'è una ragionevole probabilità che maggiori restrizioni sulla diffusione di informazioni sensibili riduce le possibilità di fughe di notizie e compromessi (“need-to-share”).

I principali moduli funzionali disponibili all’interno del servizio IAM fornito sono:

- **Identity Management & Governance**: è responsabile per la gestione del ciclo di vita delle identità digitali, gestisce la creazione, la modifica o la cancellazione delle identità, i loro attributi e il rapporto tra identità e attributi all'interno del sistema IAM. Inoltre, è responsabile per la gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestite le risorse di amministrazione;
- **Access Control & Management**: è responsabile di gestire l'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali;
- **Credential Management**: è responsabile per la gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.;
- **Multi Factor Authentication**: gestisce gli schemi di autenticazione utilizzati sul sistema IAM multifattore (gestione delle password, OTP Token, Smart Card, etc.). Per garantire la sicurezza dell’intera filiera applicativa il sistema di autenticazione multi-fattore deve garantire i livelli di sicurezza definiti all’interno della norma ISO/IEC DIS 29115
- **Logging & Reporting**: è il componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema IAM per generare rapporti per uso amministrativo o di revisione contabile;
- **Federation Services**: rappresentano i servizi di federazione verso Identity Provider Esterni garantendo la piena compatibilità con i più diffusi sistemi di autenticazioni federati (SPID, eIDAS, CNS, etc.). In particolare, con l’introduzione dello SPID (Sistema Pubblico di Identità Digitale) promosso dall’Agenzia per l’Italia Digitale (AgID), il servizio proposto consente di accedere con un unico login ai diversi servizi on line di tutti i Soggetti Pubblici (PA) e Privati che adottano questo sistema di autenticazione. Il servizio SPID Enabling consente di connettere e abilitare i servizi web di aziende pubbliche e private al sistema di autenticazione SPID (Sistema Pubblico delle Identità Digitali) basandosi su un gateway di federazione SAML 2.0 nel quale sono state implementate le logiche e le specifiche tecniche SPID ed abilita ad un sistema di autenticazione federato verso tutti gli Identity Provider accreditati AgID.

### 2.4.3 Big Data

Il servizio consente la costruzione di Data Lake as a service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale e un servizio per la data governance:

- **Data Lake**



TIM - Uso Interno - Tutti i diritti riservati.

Questa soluzione PaaS fornisce una piattaforma pronta all'uso che dispone di tutte le funzionalità necessarie a sviluppatori, Data Scientist e analisti per archiviare facilmente dati di tutte le dimensioni, forme e velocità.
Tale soluzione permette l'archiviazione e analisi di file con scalabilità orizzontale, lo sviluppo di programmi con architettura altamente parallela, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes), essere progettato per essere utilizzato su infrastrutture cloud e supportare una vasta gamma di linguaggi (Python,R, Java, .Net, Scala).

- **Batch/Real time Processing**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso per sviluppare processi batch e in streaming basati su un motore di esecuzione in Memory e basato su scalabilità orizzontale e parallela. Tale soluzione consente l'analisi di grandi moli di dati sia in batch che in streaming, un paradigma di programmazione unico per l'analisi in batch e in streaming, lo sviluppo di programmi performanti con utilizzo di architetture scalabili orizzontalmente e parallele, mette a disposizione Tool per il Debug e l'ottimizzazione dei programmi sviluppati, è Integrabile con Schedulatori di Risorse Esterni (YARN, Kubernetes) e cloud ready, supporta una vasta gamma di linguaggi (Python,R, Java, .Net, Scala), espone api rest per il monitoraggio e il submit dei job da remoto, fornisce un pannello per il monitoraggio del job e dettagli per singolo job, integrabile con Storage Esterni (Data Lake Paas), fornisce funzionalità di autoscaling e fornisce meccanismi di caching su SSD.

- **Event Message**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per sviluppare applicazioni e pipeline dati in real time inoltre deve fungere da Message Broker fornendo funzionalità di tipo Publish e Subscribe.
  Tale soluzione permette la gestione di grandi moli di eventi, lo sviluppo di programmi basati su architettura altamente parallela e scalabile orizzontalmente, fornire tool per il Debug e l'ottimizzazione dei programmi sviluppati, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes) e progettato per essere utilizzato su infrastrutture cloud, supportare una vasta gamma di linguaggi (Python, R, Java, .Net, Scala), fornire funzionalità di autoscaling, implementare meccanismi di consegna degli eventi in ordine ed essere integrabile con framework di Stream Processing (Spark).

- **Data Governance**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso che mette a disposizione un unico punto di riferimento sicuro e centralizzato per il controllo dei dati. Sfruttando strumenti di "search and discovery" e i connettori per estrarre metadati da qualsiasi sorgente di dati, permette di semplificare la protezione dei dati, l'esecuzione delle analisi e la gestione delle pipeline, oltre ad accelerare i processi ETL.
  Tale soluzione consente di analizzare, profilare, organizzare, collegare e arricchire automaticamente tutti i metadati, implementare algoritmi per l'estrazione di Metadati e relazioni in modo automatico, supportare il rispetto delle normative e della privacy dei dati con il tracciamento intelligente della provenienza dei dati (data lineage) e il monitoraggio della conformità, semplificare la ricerca e l'accesso ai dati e verificare la validità prima di condividerli con altri utenti, produzione di dati relativi alla qualità del dato, definire in modo semplice e veloce i modelli e le regole necessarie per validare i dati e risolvere gli errori,



TIM - Uso Interno - Tutti i diritti riservati.

permettere di supervisionare gli interventi per la risoluzione degli errori dei dati e mantenere la conformità rispetto a audit interni e normative esterne.

### 2.4.4 Artificial Intelligence

Il servizio mette a disposizione un set di algoritmi preaddestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning:

- **AI Platform**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per costruire modelli di ML/DL facilitando l'accesso al dato mettendo a disposizione una ambiente collaborativo a cui partecipano sia esperti di contesto che Data Scientist.
  Tale soluzione permette il supporto di almeno le seguenti tipologie di sorgenti dati: NoSQl, SQL, Hadoop File Formats, Remote Data Sources, Cloud Object Storage, Cluster Hadoop, Rest Api; fornisce moduli configurabili per il data cleaning, wrangling e mining, strumenti e librerie per la visualizzazione dei dati, supporta le principali librerie per lo sviluppo di modelli di ML/DK (PyTorch, TensorFlow, ScikitLeran, H20,XGBoost, etc), supportare gli ultimi trend tecnologici (AutoML, Explanable AI), supportare una vasta gamma di linguaggi (Python, R) e strumenti a Notebook (Jupyter), permette la gestione della sicurezza di livello enterprise con la possibilità di implementare politiche RBAC, fornisce un approccio visuale di tipo Drag&Drop per lo sviluppo, la gestione intera del ciclo di vita di un progetto di datascience (Business Undestanding, Data Acquisition&Understanding, Modeling, Deployment), rende possibile interrogare i modelli attraverso degli endpoint Rest, monitorare le performance dei singoli modelli, supporta sia CPU che GPU, permette il Deploy dei modelli in versione dockerizzata e su Kubernetes, permette la creazione di pipeline di automation per la creazione di ambienti e il rilascio dei modelli, permette la creazione di Wiki per la condivisione delle informazioni relative ai singoli progetti, è integrabile con IAM esterni, permette il tracciamento e monitoraggio di tutte le azioni effettuate sulla piattaforma, permette la gestione centralizzata delle risorse di computing, permette la possibilità di creare policy custom per la protezione del dato e integrabile con sistemi di calcolo distribuiti (Spark, Hive, Impala, etc).

- **Semantic Knowledge Search**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di rendere facilmente accessibili le informazioni contenute all'interno del patrimonio informativo (documenti, immagini, video) utilizzando un motore di ricerca semantico in grado di interpretare richieste in linguaggio naturale.
  Tale soluzione permette di gestire contenuti in varie tipologie di formati (Documenti Word, pdf, pptx , email, immagini, video, etc), di indicizzare le informazioni contenute nei documenti, l'implementazione di un motore di ricerca di tipo full-text e di tipo semantico performante, l'esposizione di un'interfaccia in linguaggio naturale, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo), implementare meccanismo di auto apprendimento mediante feedback utenti, garantire la sicurezza del dato con vari tipologie di protezione (At rest, In Transit), garantire scalabilità orizzontale, esporre delle api per l'integrazione con sistemi esterni e essere integrabile con uno IAM esterno.



TIM - Uso Interno - Tutti i diritti riservati.

- **Text Analytics /NLP**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso in grado di estrarre informazioni da testo non strutturato.
  Tale soluzione consente di esporre delle api rest per l'inferenza dei modelli, l'estrazione di Entità dal testo (Persone, Luoghi, etc), estrazione di concetti chiave dal testo, estrazione del Sentiment, riconoscimento della Lingua, garantisce scalabilità orizzontale, supporto Load Balancing, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo),il tracciamento e il monitoraggio delle interrogazioni al sistema e la possibilità di essere eseguibile su Kubernetes o in versione dockerizzata.

- **Audio Analytics**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti audio.
  Tale soluzione permette di analizzare grandi volumi di audio, garantire scalabilità orizzontale, supportare Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni da fonti audio (Analisi rumore ambientale, Speaker Identification, Audio Insight), esporre un'interfacciata basata su api rest per l'inferenza, permettere la configurazione degli algoritmi da User Interface, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generazione di Eventi verso sistemi esterni, elaborazione sia in streaming che in batch, algoritmi estendibili attraverso componenti dockerizzate e deployable su Cluster Kubernetes.

- **Video Analytics**
  Piattaforma PaaS pronta all'uso in grado di applicare algoritmi basati su AI su fonti video.
  Tale soluzione consente di analizzare grandi volumi di video, garantire scalabilità orizzontale, supporto al Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni dai video (Detection, Classification, Identification, Counting, Density Estimation), esporre un'interfacciata attraverso api rest per la lettura dei metadati generati dagli algoritmi, fornire un portale web per la configurazione dei flussi video e degli algoritmi, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generare Eventi verso sistemi esterni, elaborazione dei video sia in streaming che in batch e fornire estendibilità degli algoritmi attraverso componenti dockerizzate.

## 2.5 BaaS e DRaaS

Proteggere le applicazioni critiche facendo leva su un servizio di backup è allo stato attuale il modo migliore per garantire la continuità operativa. È fondamentale impostare per tutte le attività, anche e soprattutto quelle mission critical, un meccanismo automatico di duplicazione dei dati utilizzati e generati nelle attività quotidiane. Questo consente, in caso di interruzioni del servizio, attacchi informatici o perdita di informazioni, di accedere ai dati salvati e ripristinare immediatamente l'operatività di tutti i sistemi, riducendo al minimo – o addirittura azzerando – il downtime.

### 2.5.1 BaaS: Golden copy protetta

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard (cfr. § 4.1.5), la NewCo PSN mette a disposizione un servizio opzionale aggiuntivo che analizza i backup



TIM - Uso Interno - Tutti i diritti riservati.

mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione.

Si tratta di una funzionalità completamente gestita ed opzionale, attivabile su richiesta, in aggiunta al servizio di Backup standard: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy; in particolare, quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul sistema sorgente e queste *signature* vengono utilizzate per convalidare i dati del backup. Una volta validate, tali *signature* vengono memorizzate con il backup stesso: ciò permette di eseguire automaticamente la verifica della consistenza dei dati salvati nel backup, utilizzando le signature salvate.

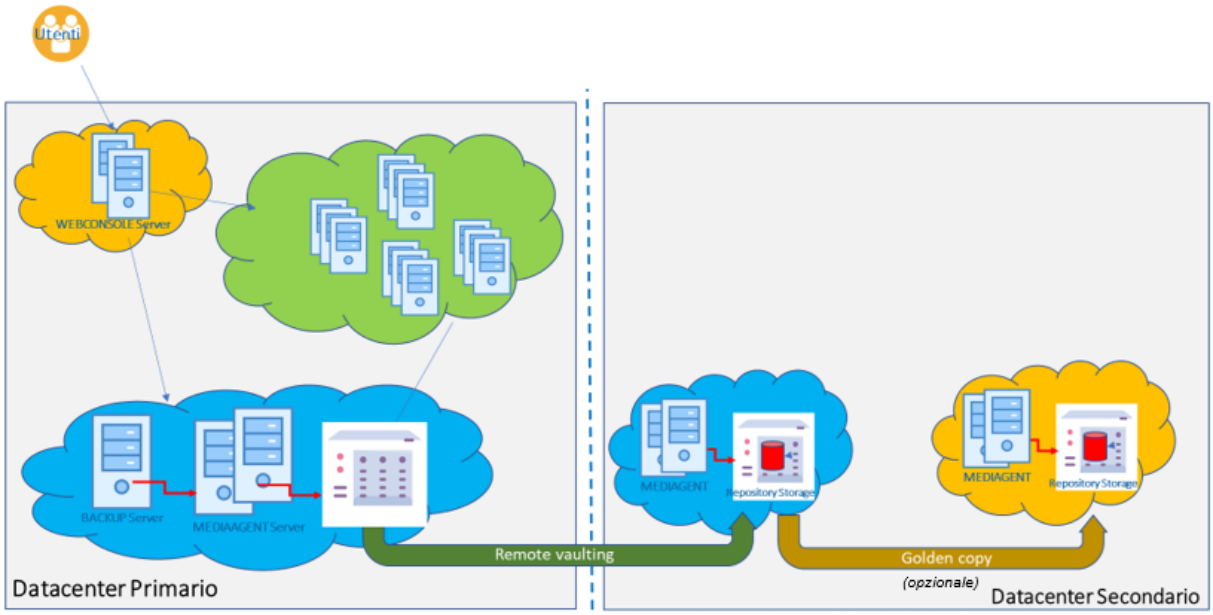



**Figura 1: Architettura Funzionale Golden Copy**

Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (*WORM: Write Once, Read Many*) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute, ecc) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali attacchi ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy.



TIM - Uso Interno - Tutti i diritti riservati.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo *ransomware* non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: Solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo *ransomware*, si potrà procedere all'archiviazione della "*golden copy*" in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

- ✓ analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di *ransomware*);
- ✓ certificazione della Golden Copy da parte della NewCo PSN;
- ✓ protezione su storage distinto di backup, **privo di ogni accesso fisico e logico;**
- ✓ replica in **Region diverse e su canale cifrato**.

### 2.5.2 DRaaS

Il Disaster Recovery "*as-a-Service*" (DRaaS) è il servizio di cloud computing che consente il ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso. Il modello *as-a-service* prevede che l'amministrazione stessa non debba essere proprietaria di tutte le risorse né occuparsi di tutta la gestione per il Disaster Recovery, affidandosi al service provider per un servizio completamente gestito. La pianificazione del Disaster Recovery è fondamentale per la Business Continuity (cfr. "Specificazione caratteristiche del servizio e della gestione"). Il DRaaS si basa sulla replica e sull'hosting dei server in un site del PSN diverso rispetto all'ubicazione primaria. Il PSN implementa un piano di Disaster Recovery in caso di evento disastroso che causa l'indisponibilità del servizio un cliente.

## 2.6 CaaS

Il **Servizio Infrastrutturale in modalità CaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura in grado di distribuire e gestire tutte le applicazioni basate su **container** in carico alla PA all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica descritti nel § **3. *Sicurezza*** e § **4. *Infrastruttura e Network.***

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

## 2.7 Security

### 2.7.1 DDOS Protection

La NewCo PSN renderà disponibile per tutte le PA che attiveranno i propri servizi all'interno dell'infrastruttura proposta un servizio di Protezione DDOS. Tale servizio di Distributed Denial as a Service (DDoS) è un servizio di sicurezza infrastrutturale che va ad aggiungersi ed integrarsi ai servizi già previsti dal presente progetto.



TIM - Uso Interno - Tutti i diritti riservati.

Il servizio di DDoS Protection proposto dalla NewCo PSN garantisce la mitigazione degli attacchi DDoS provenienti esclusivamente da rete Internet e diretti ai sistemi delle Amministrazioni ubicati nei Centri Servizi previsti dal progetto.

La tipologia di attacco contrastata dal servizio offerto è il "Volumetric Attack" che mira alla saturazione del link di collegamento mediante la generazione di altissimi volumi di traffico e rendendo indisponibile il sistema del Cliente. Tale tipologia di attacco è generalmente generata da:

- botnet (reti di computer/server compromessi mediante malware e in possesso degli attaccanti),
- server in hosting con alta capacità di generazione traffico in banda,
- server/servizi che vengono abusati per generare traffico anomalo sfruttando debolezze dei protocolli esposti (DDoS Relection & Amplification),
- redirezione di traffico di navigazione da client leciti mediante compromissione di siti e banner pubblicitari,
- infrastrutture DDoSaaS (Distributed Denial of Service as a service anche dette Booter/Stresser) che consentono di lanciare attacchi di diversa tipologia previa pagamento di un abbonamento).

Il contrasto efficace di questo tipo di attacchi, per la loro stessa natura, può essere realizzato esclusivamente proteggendo le risorse trasmissive che forniscono la connettività Internet. Nel caso di attacchi DDoS la protezione risulta tanto più efficace quanto più è realizzata in prossimità delle sorgenti degli attacchi e quindi lontano dai target. Per tale motivo una protezione ottimale può essere realizzata solo ed esclusivamente nell'infrastruttura dell'operatore di TLC che fornisce il servizio di connettività.

Il servizio proposto è basato su una soluzione "surgical mitigation", ovvero una protezione che agisce esclusivamente sul traffico destinato al singolo IP attaccato e non su una soluzione "carrier agnostic", che per gestire una un attacco deve detenere completamente almeno una /24. La protezione "surgical mitigation" è sempre attiva ed efficace, mentre quella di tipo "carrier agnostic" risulta efficace solo in caso di attacchi realizzati puntando a risorse tramite un nome (FQDN - fully qualified domain name), sfruttando una redirezione basata su DNS non proteggendo nel caso di un attacco all'indirizzo IP assegnato alla risorsa.

Il servizio è applicabile esclusivamente alla connettività Internet condivisa fornita dalla NewCo PSN presso i propri Centri Servizi ed utilizzata dalle Amministrazioni che contrattualizzeranno i servizi infrastrutturali previsti dal presente progetto. Nello specifico il servizio DDoS Protection protegge esclusivamente IP pubblici esposti su Internet da attaccanti che siano in Internet, pertanto eventuali attacchi provenienti dalla rete INFRANET non sono né rilevabili né gestibili. Il servizio non è applicabile alla connettività INFRANET poiché quest'ultima è realizzata mediante una VPN MPLS.

Il servizio di DDoS Protection offerto prevede una gestione "proattiva automatica" con copertura H24. L'attività di contrasto ad un attacco di tipo DDoS è composta da tre fasi distinte:



TIM - Uso Interno - Tutti i diritti riservati.

- Diversion
- Cleaning
- Re-injection

La figura seguente mostra lo schema generico di funzionamento del servizio in caso di attacco.

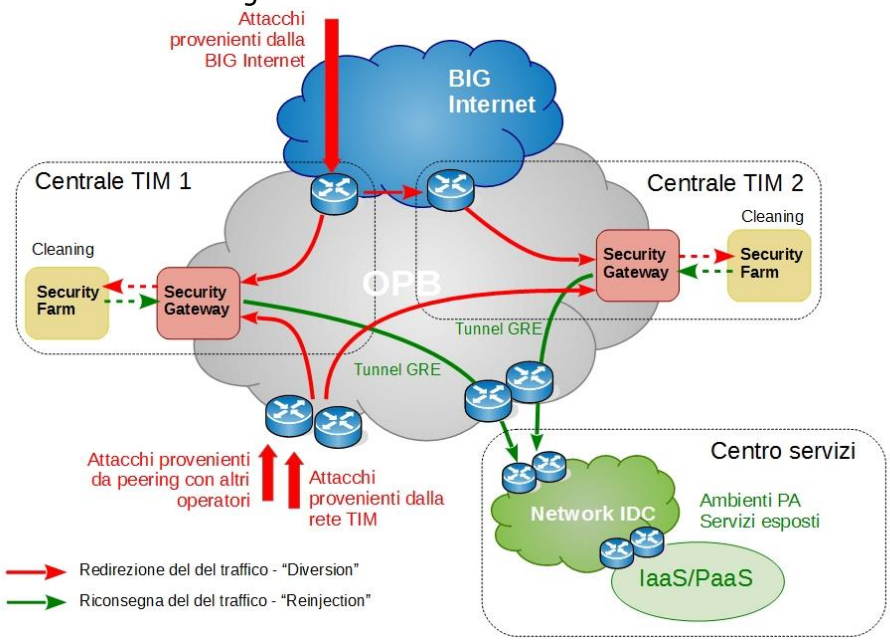



**Figura 2: Rappresentazione dell'architettura di prevenzione del DDoS in presenza di attacchi**

Di seguito sono dettagliate le tre fasi sopra indicate:

- Diversion: Il Security Operation center (SOC) attiva la redirezione del traffico Cliente riferito all'IP o agli IP sotto attacco verso le Security Farm con l'obiettivo di analizzare i flussi di traffico sotto attacco e intraprendere le azioni di cleaning.
- Cleaning: A seguito della diversion, il traffico è consegnato all'apparato di cleaning che analizzerà la tipologia dell'attacco e applicherà tutte le misure necessarie ad eliminare la sola componente indesiderata del traffico. Al termine delle attività di pulizia, il solo traffico legittimo è riconsegnato al Cliente attraverso la funzionalità di Re-Injection.
- Re-Injection: Il traffico legittimo viene riconsegnato al Cliente attraverso un tunnel GRE chiuso tra le Security Farm ed i router di attestazione del centro servizi che ospita i sistemi oggetto di attacco. Nello specifico il tunnel verrà chiuso sul router infrastrutturale del Centro Servizi presso cui sono posizionati i sistemi Cliente sul quale è terminata la connettività Internet. La modalità Tunnel GRE assicura che il traffico sia instradato in maniera puntuale.

### 2.7.2 Servizi Professionali di Sicurezza

Il PSN offre molteplici strumenti per gestire la sicurezza dei dati delle Amministrazioni e mitigare i rischi che tali dati vengano sottratti, rubati, modificati o distrutti. Rendere disponibili infrastrutture



TIM - Uso Interno - Tutti i diritti riservati.

intrinsecamente dotate di un livello di sicurezza elevato, di per sé non è sufficiente a garantire la completa sicurezza delle informazioni ivi trasferite. Questo principalmente per una serie di motivi tra cui:

- requisiti normativi cogenti di natura cyber/privacy;
- mancanza di flessibilità nella stipula dei contratti;
- mancanza attuale di pubblicazioni o risposte in merito alla conformità a standard applicabili per la normativa italiana;
- scarsa conoscenza della nuova tecnologia e conseguente sottovalutazione dei rischi di migrazione;
- necessità di ridisegnare le architetture e i controlli di sicurezza, in quanto quelli utilizzati in ambienti tradizionali spesso non risultano efficaci in ambienti cloud o multicloud;
- difficoltà e complessità a mantenere centralizzato il governo dei processi e le tecnologie di sicurezza, anche e soprattutto in scenari multicloud ibridi;
- poca conoscenza e conseguente difficoltà ad abilitare e sfruttare i seppur efficaci strumenti di sicurezza nativi dei cloud provider;
- difficoltà di gestire i processi di audit e gestione degli incidenti, soprattutto in casi di analisi post-mortem e forense.

In conseguenza di tutte le problematiche sopra evidenziate vengono proposti servizi professionali per affiancare le Amministrazioni nell'implementare le opportune contromisure all'interno del proprio ambiente cloud.

#### 2.7.2.1 *Ambito di attività*

I servizi professionali relativi agli ambiti di sicurezza erogati dal PSN saranno a disposizione delle Amministrazioni per tutte quelle attività necessarie ad aumentare il livello di sicurezza e a mitigare i rischi, tra cui:

- supporto all'allineamento della strategia di sicurezza alla strategia di migrazione;
- assessment delle minacce e delle vulnerabilità del AS-IS;
- redazione del documento di gap analysis dei controlli di sicurezza in ottica di architettura target (TO-BE);
- supporto all'implementazione dei controlli e delle policy di sicurezza;
- assessment delle vulnerabilità dell'architettura target;
- supporto all'analisi del rischio e alle verifiche di conformità;
- attività di Audit/Pre-audit.

Durante la fase di migrazione, sulla base del livello di sicurezza richiesto e della sensibilità dei dati migrati, i servizi professionali potranno fornire il supporto necessario all'implementazione dei controlli, allo scopo di attivare i servizi richiesti dalla PA, tra cui:



TIM - Uso Interno - Tutti i diritti riservati.

- cifratura dei dati “In motion” (traffico di rete di risorse esposte e non esposte) e “At rest”;
- gestione delle chiavi di cifratura;
- definizione di policy per il controllo degli accessi per tutte le tipologie di utenze degli ambienti cloud (applicative, nominali, amministrative) secondo il principio del “Least Privilege”;
- valutazione e configurazione di Password Policy;
- rilevazione continua delle configurazioni di “default”;
- rilevazione e monitoraggio continuo degli accessi alle risorse cloud e delle chiavi di accesso;
- adozione di utilizzo di tecniche di autenticazione a 2 fattori (2fa) e di meccanismi di Single Sign On (SSO);
- messa in sicurezza degli endpoint (Antimalware, HIPS, Data Loss Prevention);
- centralizzazione degli eventi di sicurezza e log e correlazione degli eventi;
- verifica del livello di logging delle applicazioni e implementazione del livello adeguato alle attività di monitoraggio, gestione incidenti e auditing;
- accesso sicuro agli ambienti Cloud tramite link dedicati e/o Virtual Network.;
- hardening dei sistemi IaaS e PaaS.

Inoltre, potranno essere richieste le seguenti attività aggiuntive:

- Vulnerability Assessment per la rilevazione delle vulnerabilità infrastrutturali, in caso di servizi di housing, hosting e IaaS;
- Static Application Security Testing per i test sul codice sorgente delle applicazioni;
- Dynamic Application Security Testing per i test sulle applicazioni in esecuzione;
- Penetration test applicativo.

I servizi sopra elencati forniranno un ulteriore livello di sicurezza, rispetto agli standard di sicurezza adottati nel perimetro del PSN descritti al paragrafo 3, che potranno essere attivati su richiesta della singola PA. L’obiettivo di tali attività è identificare, classificare e mitigare i rischi e le vulnerabilità all’interno del perimetro di servizio della singola Amministrazione.

Per ogni progetto verrà individuata il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste.

## 2.8 Refresh tecnologico

Di seguito la descrizione della modalità di gestione del refresh tecnologico.
L’architettura Cloud è basata sulla integrazione tecnologica di componenti HW e SW che hanno un determinato ciclo di vita garantito dalle roadmap dei diversi HW/SW Vendor. Partendo da



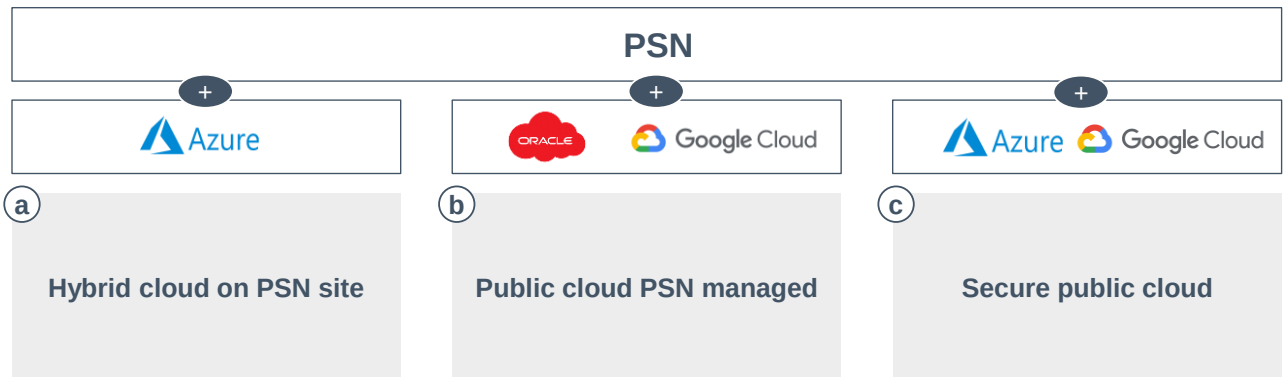
TIM - Uso Interno - Tutti i diritti riservati.

questo presupposto, si prevede per l'architettura Cloud (incluso il servizio di Hosting) un ciclo di vita di circa 5 anni relativamente alle componenti HW (fondamentalmente computing layer).
A fronte di una dichiarazione di End of Support/Life dallo specifico HW Vendor, si procederà alla valutazione delle componenti di nuova generazione da integrare nell'architettura, all'integrazione nel perimetro di servizio e alla successiva sostituzione di quelle in servizio.
Dal punto di vista del SW, invece, il processo prevede il mantenimento dello stato dell'arte attraverso l'implementazione degli aggiornamenti forniti dai relativi SW Vendor, seguendo le procedure che saranno definite dalla NewCo PSN che permetteranno di mantenere la continuità di servizio.
In caso di annuncio di End of Support/Life per un prodotto, si procederà all'analisi e allo studio di fattibilità per giungere alla implementazione di una nuova versione SW. Tale attività prevede anche la validazione da parte della funzione Security al fine di garantire il più alto livello di sicurezza che sarà garantito dalla NewCo PSN.
Tali aggiornamenti, soprattutto quelli SW, trattandosi di attività che riguardano il livello infrastrutturale della piattaforma Cloud sottesa all'erogazione del servizio per le PA, potrebbero avere degli impatti sulle VM/Applicazioni della PA e quindi, in ogni caso, ogni singolo refresh tecnologico, HW o SW che sia, verrà verificato con i referenti della PA qualora comportasse necessari requisiti anche lato VM/Applicazioni e quindi potenziali modifiche preventive da parte del cliente finale.

## 2.9 Il ruolo dei CSP

La NewCo PSN, oltre a rendere disponibili servizi Cloud che erogherà da un'infrastruttura realizzata appositamente per il seguente progetto, offrirà ulteriori servizi cloud avvalendosi della collaborazione dei principali Cloud Service Provider (CSP).

La PA tramite il PSN potrà accedere in piena sicurezza e sovranità ai servizi dei CSP in funzione dei suoi bisogni e in modalità Private, Hybrid e Public.




Nello specifico i servizi che verranno descritti nei successivi paragrafi vedono il coinvolgimento di Google, Microsoft ed Oracle.



TIM - Uso Interno - Tutti i diritti riservati.

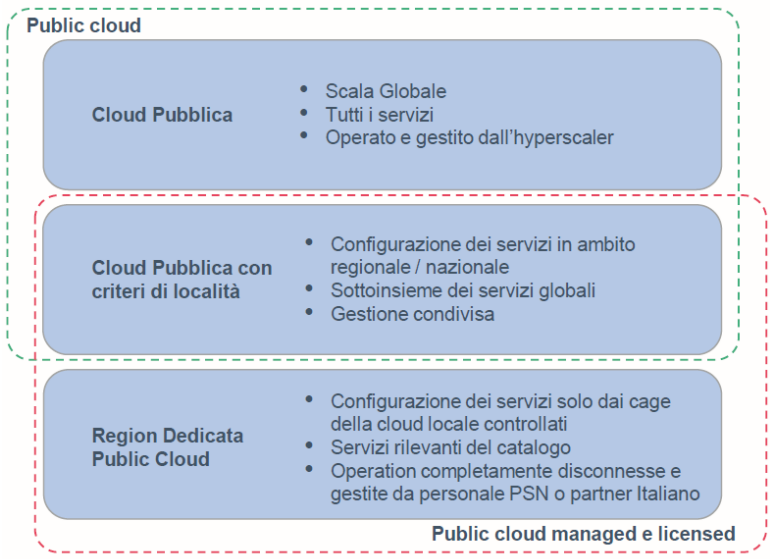
### 2.9.1 Public Cloud PSN Managed

A seguire un overview sul Public Cloud PSN Managed i cui dettagli sono descritti nel proseguio del paragrafo.

Il Public Cloud PSN Managed permetterà alle PA di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica e gestione operata da personale PSN.



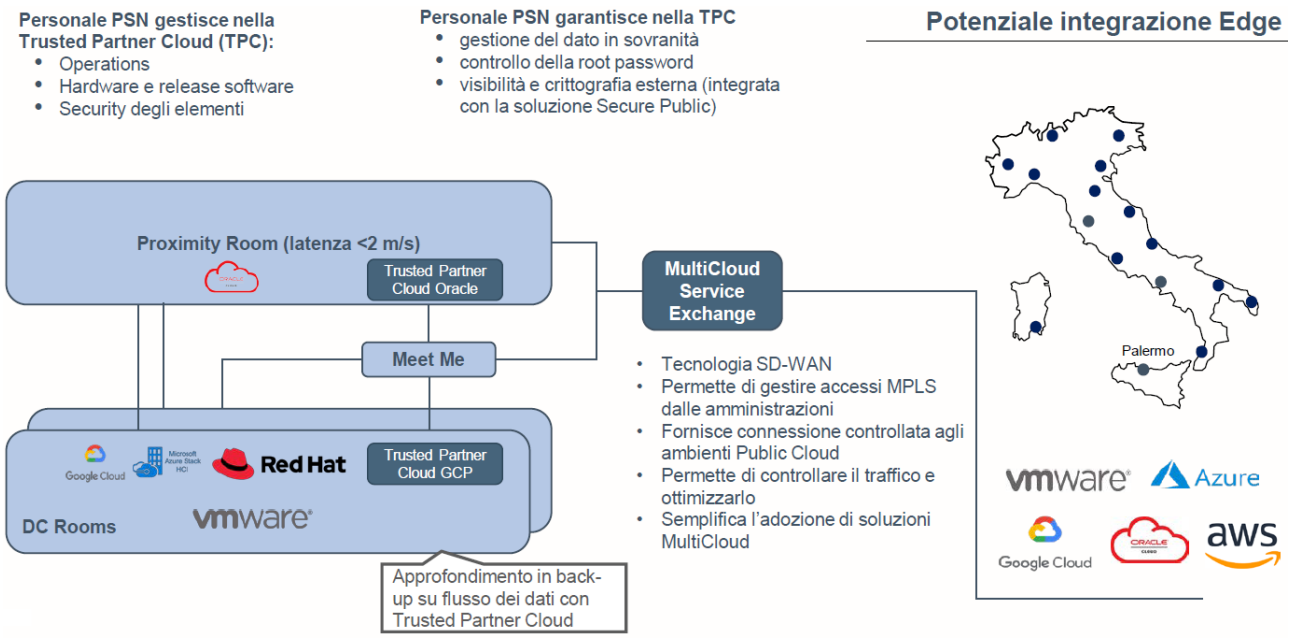

Relativamente al modello di servizio Public Cloud PSN Managed, nella prima figura vengono messe in risalto le **differenze e integrazioni con il modello Public Cloud puro in Region Italiana**; nella seconda se ne descrive **l'architettura e l' interconnessione.**




- **Partner di fiducia**: TIM partner italiano, formato su tecnologia di base GCP e Oracle
- **Ispezione dei controlli:** personale PSN e/o di TIM ispeziona l'implementazione e il funzionamento dei controlli di Google e Oracle. Ciò include audit del codice, l'accesso alla telemetria di sicurezza e strumenti per applicare e monitorare l'implementazione dei controlli dei propri clienti su Google Cloud
- **Approvazione del Partner**: alcune classi di accesso amministrativo ai dati, implementazioni di sistemi critici, deploy e modifiche del codice, modifiche operative richiederanno un LGTM esplicito da parte del partner per il completamento
- **Root of Trust esterna:** il partner controlla la root of trust per tutti i dati dei clienti. In caso di comportamento reputato non appropriato da parte degli hyperscaler (Google e Oracle), il partner potrà revocare l'accesso alla gestione delle infrastrutture



TIM - Uso Interno - Tutti i diritti riservati.




Il Servizio di Public Cloud PSN Managed è basato sulle tecnologie e i servizi cloud degli Hyperscaler Google ed Oracle e quindi sulle relative piattaforme Google Cloud Platform (GCP) e Oracle Cloud: tali servizi sono gestiti completamente dal personale della NewCo PSN o dei Soci, ed erogati da Data Center del PSN, quindi in territorio italiano, presso cui vengono rilasciate delle *Region* di tali piattaforme dedicate esclusivamente all'erogazione dei servizi verso la Pubblica Amministrazione.

**GCP (Google Cloud Platform)**

Per quanto concerne Google, la soluzione prevede all'interno della Region Italiana di Google, realizzata nei Data Center di TIM, un'area dedicata e segregata e gestita totalmente da personale della NewCo PSN o dei Soci. La gestione di tali servizi include in particolare le seguenti aree di attività:

- Segregazione Sicurezza di Rete;
- Segregazione livello dei dati;
- Gestione dei rilasci del software GCP verso la NewCo PSN;
- Implementazione del sistema di monitoraggio e analisi dei costi e dei consumi;
- Gestione, sostituzione e dismissione dei componenti hardware dell'infrastruttura sottesa dai servizi;
- Isolamento e monitoraggio delle aree di esecuzione tra GCP Pubblico e area PSN Managed.

**Oracle Cloud**

Per quanto concerne Oracle, la soluzione nativa è realizzata sul modello di *Oracle Region Dedicated*. L'architettura prevede una modularità in grado di sfruttare sia singoli componenti tecnologici dedicati (es. x86 systems, Exadata appliance, ecc), sia l'intera Region, in contiguità con la Region Google.

La gestione di tali servizi include in particolare le seguenti aree di attività:



TIM - Uso Interno - Tutti i diritti riservati.

- Segregazione Sicurezza di Rete;
- Segregazione livello dati;
- Gestione dei rilasci del Software Oracle Cloud;
- Implementazione della Gestione dei Costi e dei consumi;
- Gestione, sostituzione e dismissione dei componenti hardware dell'infrastruttura sottesa dai servizi, in modalità Escorted con personale Oracle e TIM.

#### 2.9.1.1 *Il servizio*

Il Public Cloud PSN Managed realizza un modello di servizio del tutto analogo al Public Cloud del CSP (o *Hyperscaler*), ma rispetto ad esso permette di implementare una logica di separazione logica e fisica, sia nella gestione operativa che nel rilascio e controllo del software di base che caratterizza il servizio.
La Region dedicata permette al personale del PSN di esercitare direttamente il controllo sui servizi del CSP, a tutti i livelli di esecuzione, per l'erogazione dei servizi dedicati alle PA:

- Hardware
- Software (gestione e rilascio in modalità quarantena)
- Rete
- Accesso e identità nella gestione

Il PSN disporrà di istanze del cloud Hyperscaler aggiungendo i propri domini, indirizzi IP, branding, fatturazione e sarà integrato con servizi di Crittografia del PSN stesso. Queste istanze possono essere totalmente disconnesse nel caso sorga la necessità' di tutelare la sicurezza nazionale.
Tale Region dedicata può essere usata per i massimi livelli di confidenzialità dei dati grazie alla sua implementazione dedicata al PSN, garantendo però allo stesso tempo tutti i vantaggi di un cloud Hyperscaler quali ad esempio elasticità', completezza di servizi, innovazione e scalabilità.

Gli attori coinvolti nella realizzazione del Public Cloud PSN Managed sono i seguenti:

- Fornitore dei servizi Cloud (CSP) che dedicherà una partizione delle proprie Region in Italia, mettendo a disposizione l'hardware, il software di gestione e l'implementazione dei servizi offerti (il CSP non potrà accedere in modo autonomo ai servizi e all'infrastruttura del PSN);
- Provider di servizi PSN (MSP-PSN).

L'MSP sarà responsabile end-to-end della gestione operativa della Region dedicata; avrà accesso esclusivo ai sistemi per l'hosting dei servizi cloud e se necessario potrà avvalersi della consulenza del CSP nella risoluzione degli *Incident*.
Le attività svolte dall'MSP includono la progettazione, l'attivazione, la gestione e il controllo dei servizi cloud, come:

- Ispezione dei controlli: possibilità di ispezionare l'implementazione e il funzionamento dei controlli del CSP. Ciò include audit del codice, l'accesso alla telemetria di sicurezza e la disponibilità di strumenti per applicare e monitorare l'implementazione dei controlli dei propri clienti sul CSP Public Cloud;



TIM - Uso Interno - Tutti i diritti riservati.

- Approvazione e autorizzazione: alcune classi di accesso amministrativo ai dati, implementazioni di sistemi critici, deploy e modifiche del codice, modifiche operative richiederanno un'esplicita approvazione da parte del PSN per la relativa attuazione;
- Root of Trust esterna: il PSN controlla la root of trust per tutti i dati dei clienti. In caso di comportamento non reputato appropriato da parte del CSP, il partner potrà revocargli l'accesso ai dati comuni.

#### 2.9.1.2 *Architettura fisica*

Il Public Cloud PSN Managed sarà implementato all'interno di una delle *Region* del PSN, prevenendo la possibilità di fornire un disaster recovery in un'ulteriore Region collocata fisicamente ad almeno 100Km di distanza dalla principale per garantire resilienza in caso di eventi di disastro. Ognuna delle Region dovrà avere almeno 3 high availability zone.

Nelle zone il CSP individuerà delle aree per isolare fisicamente gli apparati dedicati al PSN, e l'MSP avra' in carico il totale controllo degli accessi a tali aree (se necessario anche inibendo del tutto l'accesso al CSP). In caso di necessità' il personale del CSP potrà accedere (ad esempio per fare degli interventi on-site), ma dovrà essere sempre accompagnato da un responsabile dell'MSP (accesso *escorted*).
Sarà possibile per l'MSP anche ispezionare gli strumenti e le apparecchiature usate per gli interventi.

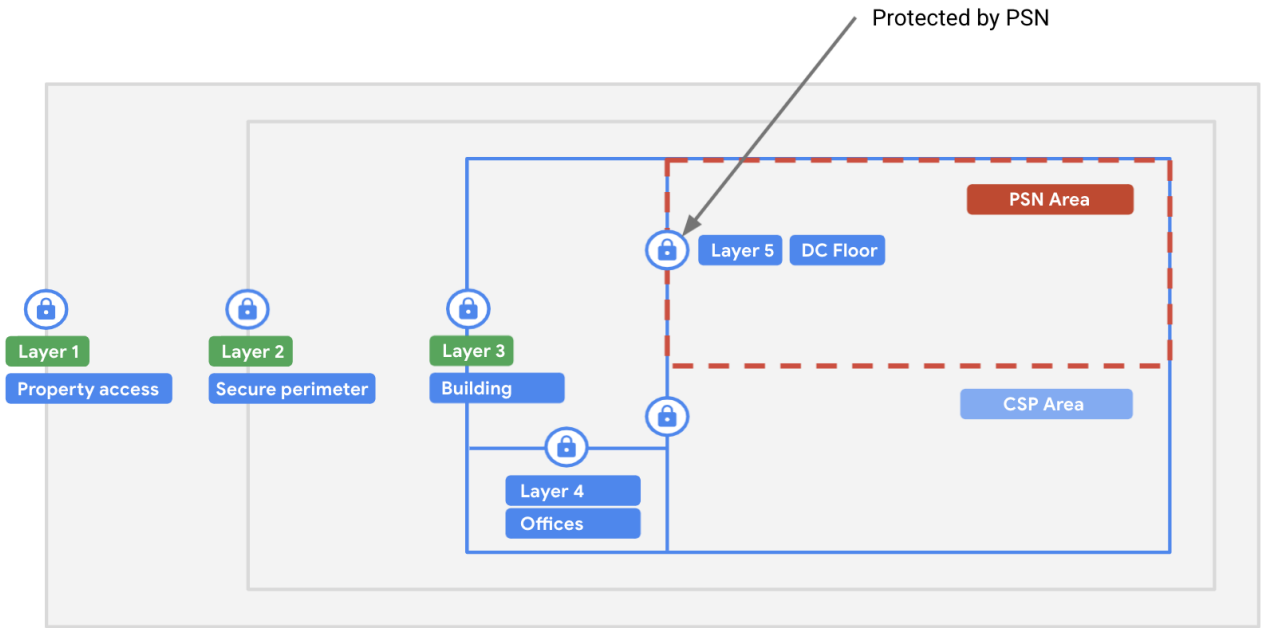



**Figura 3: Livelli di segregazione**



TIM - Uso Interno - Tutti i diritti riservati.

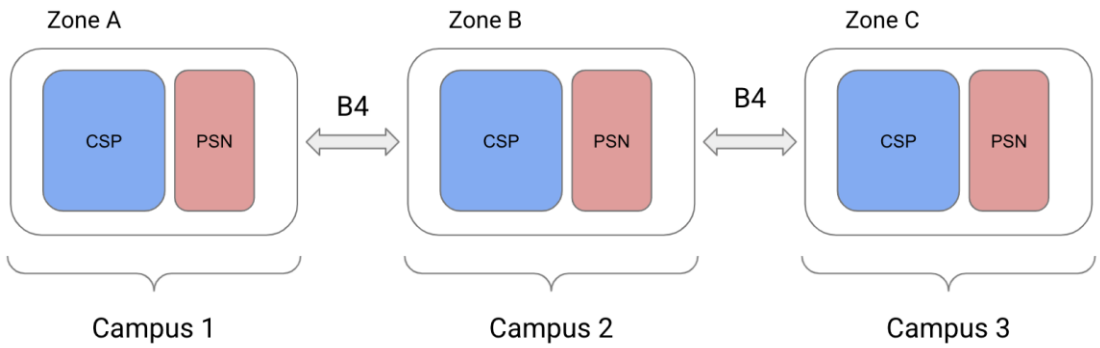



**Figura 4: Isolamento fisico delle aree dedicate al PSN**

### 2.9.1.3 *Ripartizione delle responsabilità*

Il modello Public Cloud PSN Managed prevede una ripartizione delle responsabilità che lascia all'MSP il pieno controllo dei *layer che vanno dalla gestione logica della rete fino alla sicurezza applicativa*.
Il CSP avrà la responsabilità di gestire il provisioning dell'HW e degli altri asset fisici e di fornire la piattaforma software per la gestione e l'implementazione dei servizi, lasciando comunque all'MSP la possibilità' di fare code *inspections* e la review delle modifiche.

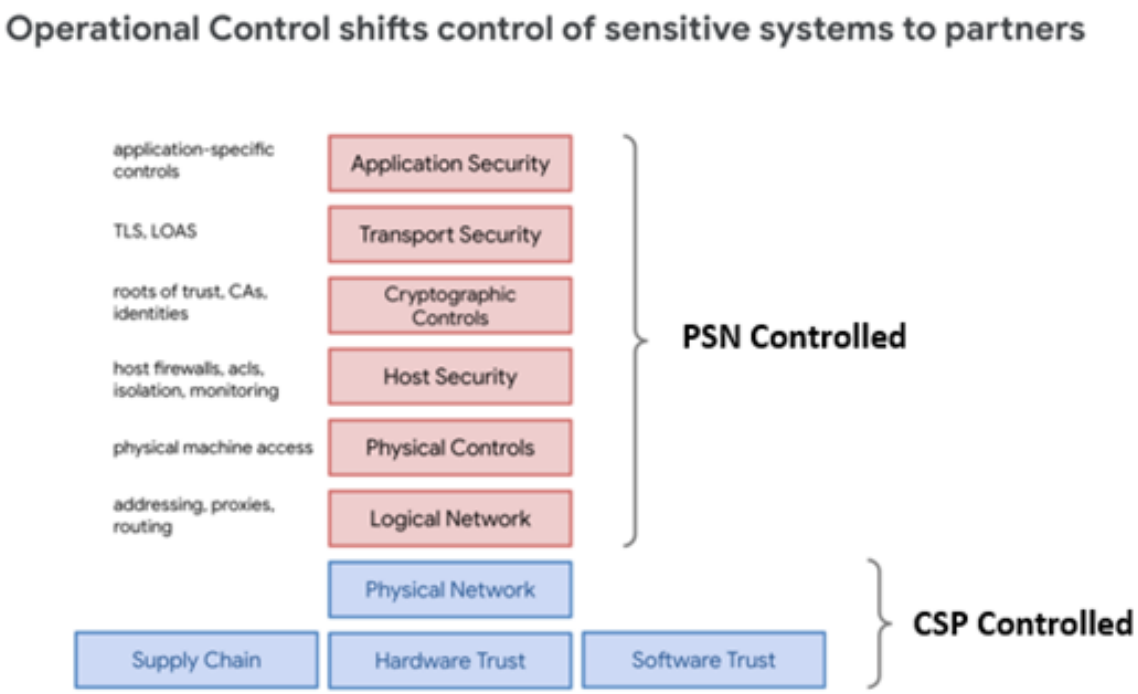



**Figura 5: Distribuzione dei livelli di Operational Control per il Public Cloud PSN Managed**

### 2.9.1.4 *Controllo della Rete*

L'MSP ha piena autonomia e totale controllo del traffico di rete da e verso il PSN. Il controllo prevede la possibilità' di ispezionare, loggare e bloccare tutto il traffico, mediante dei control proxy



TIM - Uso Interno - Tutti i diritti riservati.

scelti da vendor certificati (e non necessariamente forniti dal CSP). Il controllo del traffico riguarderà sia i dati (payload) che il traffico per il controllo e l'amministrazione. Tutto ciò a garanzia della totale copertura del rischio di data extrafiltration e di accessi non autorizzati ai sistemi.

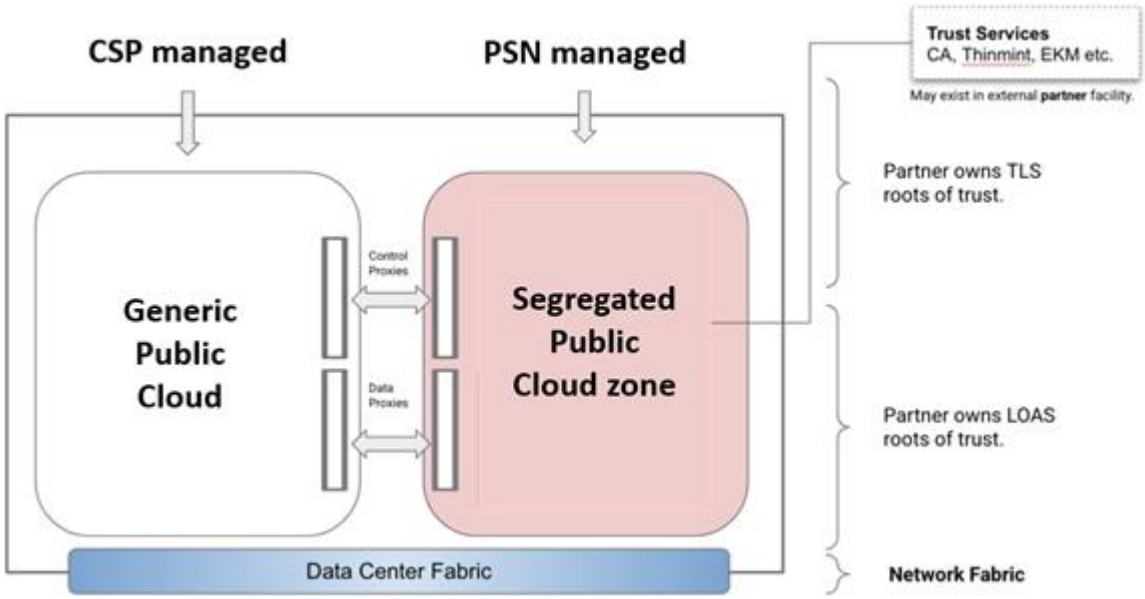



**Figura 6: Aree di intervento del PSN per il Public Cloud PSN Managed**

### 2.9.1.5 *Accesso verso l'esterno Frontend*

L'MSP fornisce, gestisce e controlla tutti gli accessi alla rete pubblica: Blocchi di indirizzi IP, peering con le reti di altri providers, ecc.
Se richiesto l'MSP potrà disporre anche di propri DNS, load balancer, VIP tunneling e strumenti di gestione aggiuntivi.
Rientra inoltre sotto il controllo dell'MSP anche tutta la gestione delle *key chains*: nomi di dominio, certificati TLS, CA, rotazione delle chiavi, scadenza, ecc.

### 2.9.1.6 *Encryption at-rest*

Tutti i dati verranno cifrati in modo trasparente *at-rested in-transit*. Le chiavi di cifratura saranno custodite dall'MSP su apparati certificati (HSM) di sua proprietà e collocati fisicamente all'esterno del perimetro controllato dal CSP. L'accesso alle chiavi custodite nell'HSM dell'MSP sarà sempre soggetto ad approvazione ed audit (sia nel caso di accesso consentito, sia nel caso di accesso negato). L'auditing dovrà avvenire su dei sistemi di persistenza che escludano il rischio di manomissione dei log (sia cancellazione che modifica). Il CSP in nessun modo avrà accesso fisico o disponibilità di utenze con privilegi di accesso all'HSM. Tutti i dati (inclusi i backup) custoditi all'interno del Public Cloud PSN Managed dovranno essere cifrati con questo meccanismo. Sarà cura dell'MSP custodire le chiavi garantendo l'alta disponibilità' e la protezione da eventuali eventi di disastro, per scongiurare l'impossibilità di poter decifrare i dati.



TIM - Uso Interno - Tutti i diritti riservati.

#### 2.9.1.7 *Gestione degli Aggiornamenti*

Tutti i CSP prevedono degli aggiornamenti frequenti sia ai servizi che ai sistemi di gestione (Continouos deployment) per rilasciare fix, nuove features o rimedi ad esposizioni di sicurezza: uno dei vantaggi del Public Cloud PSN Managed consiste proprio nel poter sfruttare questi benefici (soprattutto la celerità nel rimediare a potenziali esposizioni di sicurezza). Allo stesso tempo però l'MSP deve tutelare il PSN da eventuali modifiche che in modo malevolo (anche senza la consapevolezza del CSP) possano mettere a rischio la sicurezza delle applicazioni o dei dati.
Un possibile meccanismo a tutela di ciò' è il seguente:

1. Il CSP pubblica dei file binari (firmati digitalmente) su un repository protetto accessibile in modo esclusivo da parte dell'MSP. Il MSP avrà modo di analizzare i sorgenti con cui sono state eseguite le build e con cui sono stati rilasciati i relativi moduli.
2. Dopo un periodo di tempo concordato, il CSP rilascia i nuovi moduli su un'ambiente isolato all'interno della Region e accessibile solo al personale preposto alle verifiche dell'MSP.
3. Il MSP esegue tutti i test di sicurezza sull'ambiente "in quarantena", analizzando ad esempio il traffico di rete per individuare eventuali anomalie e flussi inattesi o sospetti.
4. A valle delle verifiche, il MSP firma i binari con un proprio certificato e approva il deployment.
5. Viene effettuato infine il deployment su ambiente di staging per ulteriori test e dopo un periodo di collaudo avviene il rilascio finale in produzione (se non vengono evidenziate anomalie)

#### 2.9.1.8 *Modello di Supporto*

Il modello di supporto prevedrà tre livelli con la seguente assegnazione di responsabilità:

- Livello 1 - L'MSP fornisce il supporto e mette a disposizione il Service desk.
- Livello 2 - Sessioni guidate. L'MSP accede ai sistemi e il CSP propone le azioni.
- Livello 3 - Il CSP accede ai sistemi, ma l'MSP segue le attività e autorizza gli accessi. Da usare solo quando c'è rischio di violazione degli SLA o in caso di emergenza.

### 2.9.2 Secure Public Cloud

Il Secure Public Cloud è un servizio che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza descritti nella documentazione tecnica (Chiavi esterne, backup, template, servizi professionali).
L'architettura del servizio "Secure Public Cloud" è basata su due componenti principali:

- **Public Cloud:** La componente **Hyperscale Public Cloud,** erogata da una *Region* collocata sul territorio nazionale, ai cui servizi vengono applicate configurazioni, policy e controlli di sicurezza, al fine di garantire ai clienti ambienti di elaborazione segregati aventi una sicurezza di base adeguata agli scopi del PSN;



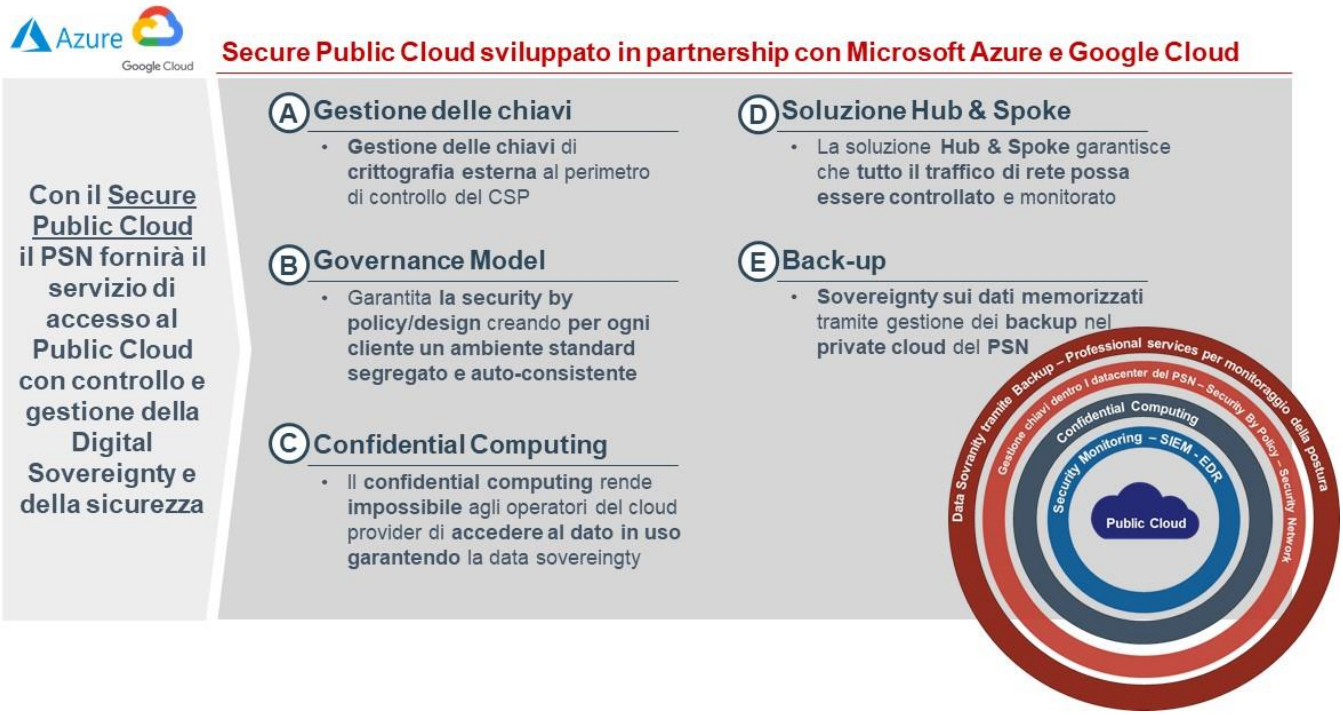
TIM - Uso Interno - Tutti i diritti riservati.

- **Security & Governance**: Una componente, erogata dal Data Center del PSN distribuiti sul territorio Nazionale, nella quale verranno configurati servizi atti a garantire l'adeguato livello di sicurezza dei servizi erogati sul Public Cloud (Gestione Chiavi e Backup).

Tale scenario prevede la presenza dei seguenti attori:

- **Fornitore dei servizi di Public Cloud** (CSP):
  - fornisce la piattaforma su cui è costruita la componente Hyperscale Public Cloud dell'architettura
- **PSN**:
  - si occupa di progettare, erogare, gestire e controllare i servizi cloud ed in modo particolare la componente di sicurezza e governo di base adeguati agli scopi del PSN;
  - fornisce servizi di sicurezza opzionali a "valore aggiunto" integrati ai servizi base tramite servizi professionali per la securizzazione.

Il Secure Public Cloud è un servizio core del PSN che garantisce alti standard di sicurezza.



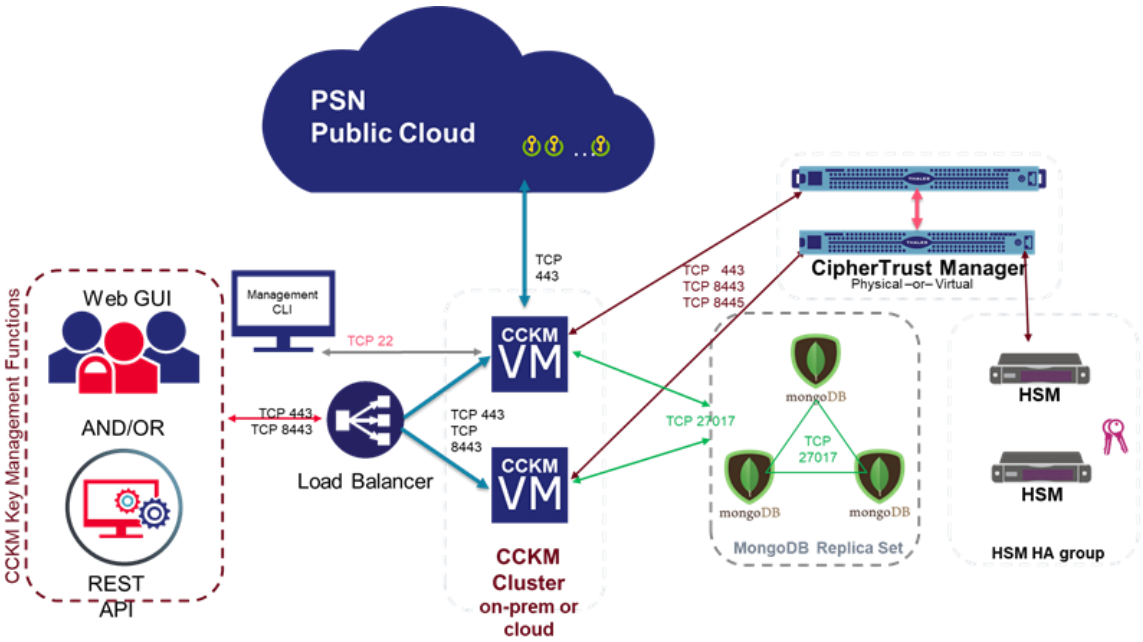

**A. GESTIONE DELLE CHIAVI**. Relativamente alla gestione delle chiavi la proposta comprende:

- Impiego di **terze parti** (e.g., Thales CipherTrust) con grande **livello di autonomia** nella **gestione delle chiavi crittografiche** per soluzioni in cloud con il modello Bring Your Own Key (BYOK).
- Soluzione di key management replicata nei due datacenter HA e territorialmente nelle due Region.
- **Controllo on-premise per ciascuna fase del ciclo vita delle chiavi**, consentendo di eseguire in autonomia:
  - generazione delle chiavi ON-PREMISE tramite l'utilizzo di dispositivi crittografici certificati;



TIM - Uso Interno - Tutti i diritti riservati.

- esecuzione dei backup delle chiavi;
- installazione diretta delle chiavi sui Key Vault in cloud;
- monitoraggio degli accessi alle chiavi;
- rotazione manuale o periodica delle chiavi;
- revoca delle chiavi.




- On-Prem HSM certificato FIPS 140-2 L3 con partizioni multiple per la corretta gestione del materiale crittografico (chiavi simmetriche ed asimmetriche, generazione entropia, ..).
- CipherTrust Manager per la gestione del ciclo di vita delle chiavi on-premise e in Cloud.
- CipherTrust Cloud Key Manager come orchestratore dei processi di gestione delle chiavi in Cloud. Generazione delle chiavi on-premise per importazione sicura sul cloud provider per tutto il ciclo di vita.

B. **GOVERNANCE MODEL.** Per ogni cliente viene **creato un ambiente standard segregato e auto-consistente** in cui, tramite servizi di delega dei privilegi (ad esempio Azure Lighthouse e Privileged Identity Management) è possibile proiettare **i servizi di monitoraggio e sicurezza dello specifico ambiente** cliente verso l'ambiente del gestore del PSN che quindi avrà:
    - Visibilità di tutti gli ambienti
    - Capacità di intervento automatizzato su larga scala
    - Possibilità di enforcement delle policy definite

**I Privilegi di amministrazione sono disabilitati** per default e vengono **attribuiti agli operatori** a valle di un processo di autorizzazione: questo meccanismo garantisce **il mutuo controllo da parte del cliente e del provider** con intrinseco innalzamento del livello di sicurezza.

Le caratteristiche di questo modello di gestione forniscono:

- Gestione uniforme e standardizzata dei tenant cliente;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, di set di regole di sicurezza predefinite in linea con best practices internazionali;



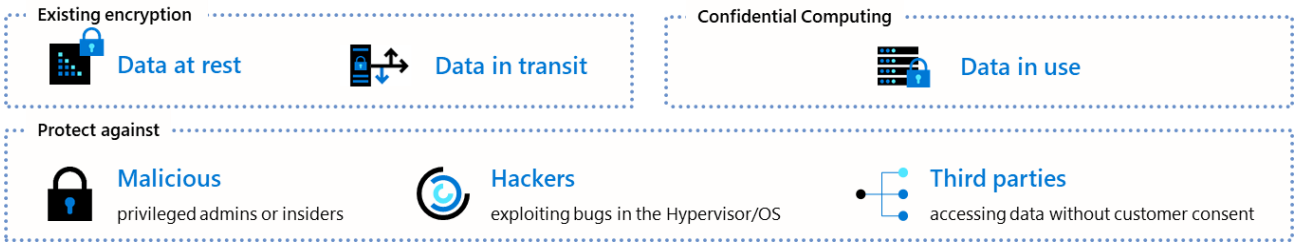
TIM - Uso Interno - Tutti i diritti riservati.

- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, dei ruoli standard per ogni funzione (Ruoli PSN, Ruoli PA, Ruoli terze parti);
- Disponibilità di template securizzati ed integrati a strumenti di sicurezza;
- Gestione unificata dell'identità;
- Gestione degli eventi di sicurezza;

C. **CONFIDENTIAL COMPUTING.** L'obiettivo del PSN è rafforzare il livello di confidenzialità e sicurezza del dato in uso tramite i seguenti metodi:
   - Ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations.
   - Usare tecniche di enforcement basate su componenti tecnologiche piuttosto che su processi organizzativi.
   - Fornire trasparenza sulle garanzie, i rischi residui e le mitigazioni che si possono implementare.

I modelli di attacco contro le applicazioni cloud si basano su tecniche diverse per prendere di mira codice o dati in uso,ad esempio:
- breakout di hypervisor e container;
- compromissione del firmware ed altre minacce interne, ognuna delle quali si basa su tecniche diverse per prendere di mira codice o dati in uso.

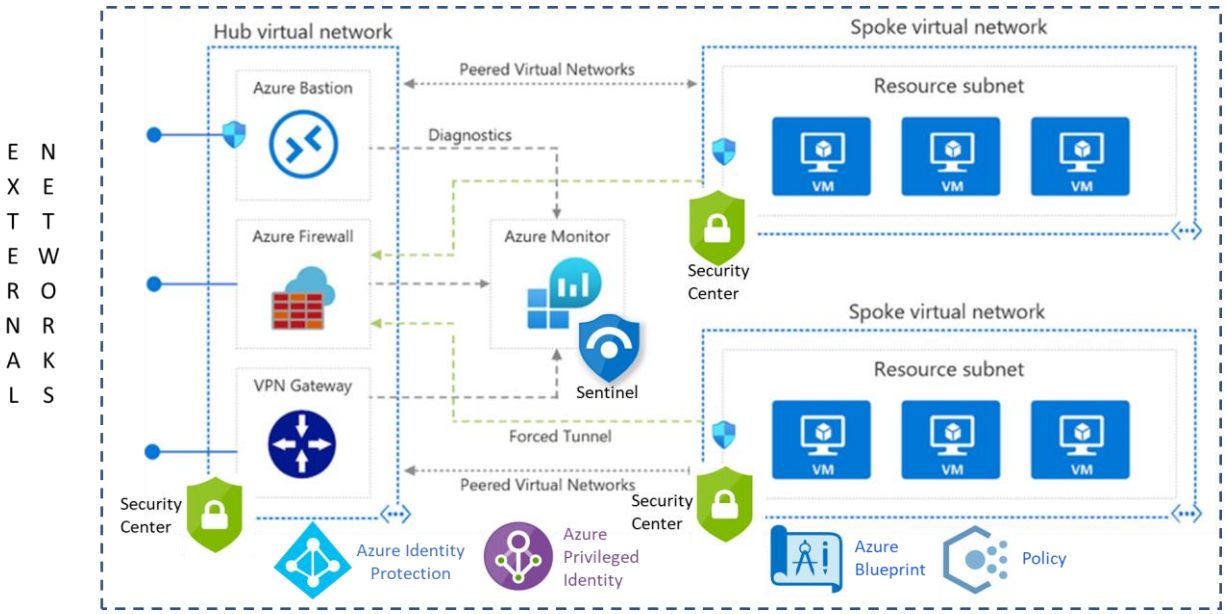
Confidential Computing (per VM, K8S, HSM) è la protezione dei dati in uso utilizzando ambienti di esecuzione attendibili basati su hardware



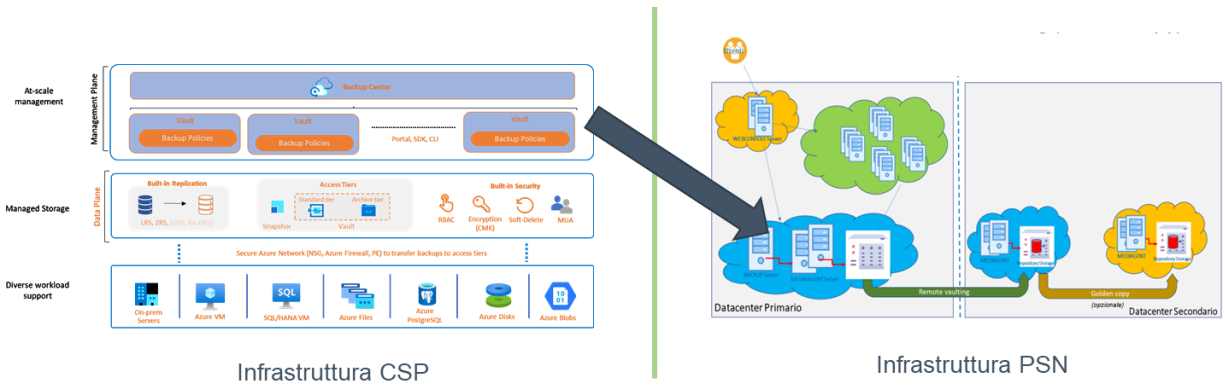

D. **SOLUZIONI HUB & SPOKE.** Per quanto riguarda l'ambiente Secure Public Cloud è previsto l'uso di un modello Hub & Spoke per consentire al PSN il controllo del traffico e la gestione delle DMZ per l'ambiente cloud.
   Le Amministrazioni potranno creare reti virtuali spoke nei segmenti, dove saranno attive Policy che forzeranno la connessione con Virtual Network Hub e impediranno la creazione di tipologie di risorse controllate centralmente, come, ad esempio, gli indirizzi IP pubblici.



TIM - Uso Interno - Tutti i diritti riservati.




**E. BACK UP.** Per esercitare la sovranità del dato, il Secure Public Cloud prevede l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP tramite ulteriore livello di archiviazione.
Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup-as-a-Service del PSN in modo che lo Storage su cui risiede il dato protetto sia gestito dal personale PSN.
L'integrazione prevede l'uso di tecniche di backup snapshot o stream-based e la cifratura dei dati "at rest" e in transito per garantire la protezione e il ripristino delle macchine virtuali a cui è rivolto il servizio, anche di quelle che implementano meccanismi di encryption del disco di sistema e dei dischi dati.




### 2.9.2.1 *Requisiti architetturali*

Per l'erogazione del servizio, devono essere soddisfatti i seguenti requisiti architetturali:

- **Il PSN è il fornitore di piattaforma**: il ruolo principale è garantire che le componenti su cui si basano i servizi offerti rispettino costantemente i requisiti di sicurezza di base. A tale fine, deve venir applicato un approccio di "visibilità" centralizzata, controllo dei servizi di sicurezza, e deployment distribuito, occupandosi di:



TIM - Uso Interno - Tutti i diritti riservati.

- definire uno specifico catalogo di servizi utilizzabili dalla PA all'interno del perimetro del Secure Public Cloud;
- definire i modelli/template degli ambienti che i clienti possono istanziare e garantirne l'*enforcement* delle configurazioni;
- implementare e controllare negli ambienti dei clienti le risorse che compongono i servizi di sicurezza di base e le policy/regole definite per la compliance degli ambienti;
- controllare la persistenza delle configurazioni e la postura di sicurezza di tutti i servizi Public Cloud del PSN.

- **Governance gestita via Policy**: gli ambiti di gestione dei vari attori sono definiti sotto forma di *Policy*, per garantire la conformità continua della piattaforma alle regole di sicurezza richieste dal PSN. Allo stesso tempo, le *Policy* consentono ai gestori sia un adeguato grado di libertà che un percorso controllato nell'adozione del modello Cloud. La governance degli ambienti deve definire regole codificate non aggirabili e/o sottoponibili a auditing per la verifica e successivo adeguamento, per creare dei confini autoritativi su tutta la piattaforma. In sintesi, le Policy garantiscono la compliance alle regole del PSN.
- **Democratizzazione degli ambiti di gestione:** il disegno non deve prevedere la centralizzazione del controllo sulle operazioni di creazione degli ambienti o delle risorse. La collocazione degli ambienti e delle risorse all'interno degli ambiti di applicazione delle policy deve garantire l'applicazione automatica delle salvaguardie native del PSN, grazie alla natura "ereditaria" delle Policy. Questo consente un ampio uso delle modalità self-service, pur mantenendo il controllo della sicurezza.
- **Change Control**: monitoraggio continuo della postura di sicurezza della PA attraverso sistemi di automazione e orchestrazione con l'obiettivo di identificare ed evidenziare modifiche che possano avere un impatto sulla sicurezza della PA, ai quali verranno sottoposte per verifica ed eventuale adeguamento.
- **Difesa in profondità:** applicando una logica a più livelli al controllo delle risorse in un sistema è possibile ridurre la probabilità che un attacco abbia successo. Infatti, un approccio al controllo delle risorse fatto a più livelli, costringe gli utenti non autorizzati ad impegnarsi per aggirare ciascun controllo, prima di poter accedere a una risorsa.
- **Verifica esplicita**: qualsiasi operazione di autenticazione o autorizzazione nella piattaforma deve validare i *data point* disponibili, quali identità dell'utente, posizione, integrità del dispositivo, servizio o applicazione, classificazione dei dati e anomalie.
- ***Least Privilege*:** l'architettura consente, in ogni sua componente, la gestione delle risorse senza l'utilizzo di privilegi persistenti, e di governare l'accesso degli utenti in modalità *just-in-time* e *just-enough-access* (JIT/JEA), nonché di attuare politiche di enforcement adattative basate sulla valutazione del rischio, al fine di garantire sia la produttività che la protezione dei dati.
- ***Assume Breach***: al fine di minimizzare gli impatti di eventuali compromissioni, occorre mantenere strettamente segregati gli ambienti dei clienti, usare servizi di cifratura del dato



TIM - Uso Interno - Tutti i diritti riservati.

e delle trasmissioni per default, e utilizzare *analytics* per ottenere visibilità e capacità di *detection* rapida e incrementare le difese e le capacità di risposta.

- ***Data sovereignty***: al fine di garantire la conservazione dei dati occorre mantenere le copie di backup delle infrastrutture e dei dati sia all'interno dello spazio dell'Hyperscaler sia conservarle all'interno dei Data Center del PSN.

#### 2.9.2.2 Architettura

L'architettura prevede due componenti primarie:

- **Servizi "Public Cloud"**: il disegno prevede l'uso dei servizi di un CSP presso cui creare un ambiente (*Tenant-Cloud*) per ciascun cliente ed uno dedicato al PSN. All'interno di ciascun *Tenant-Cloud* dei clienti finali sarà definita un'architettura a "segmenti" a cui saranno applicate *Policy* coerenti con il tipo di applicazioni che il segmento deve ospitare. La gestione operativa di questi segmenti sarà delegata con una logica di tipo RBAC, che consente la definizione di un modello i cui ruoli potranno essere assegnati al cliente finale. Sarà definito anche un segmento "speciale" (*Core*) in cui saranno attivate le risorse necessarie al controllo e all'enforcement della postura di sicurezza del cliente, il cui controllo sarà appannaggio del MSP-PSN. Come detto, su tutti i segmenti, e a diversi livelli, saranno applicate le *Policy* che garantiscono la coerenza del PSN con il modello di sicurezza richiesto per tutte le risorse definite, indipendentemente dai tempi di deployment.
  Si prevedono come necessari le seguenti componenti:

  - ***Confidential Computing:*** L'uso dei servizi del Secure Public Cloud richiederà la cifratura del dato e del traffico per default. Per applicazioni che gestiscono dati è necessario avere un controllo più stringente della catena di *trust* ed occorrerà usare meccanismi di cifratura cosiddetti "*in use*", quali il *Confidential Computing*. Il servizio di Secure Public Cloud deve essere fornito da Data Center realizzati sul territorio Nazionale.
  - ***Cifratura e gestione delle Chiavi:*** le regole del PSN richiedono la cifratura dei dati at-rest e in-flight, sia per applicazioni "convenzionali" che per quelle che richiedono controlli più stringenti; si farà quindi uso di servizi di Key Management presenti nell'ambiente Cloud che consentiranno la gestione del ciclo di vita delle chiavi in maniera integrata con l'analogo servizio implementato On-premise dell'infrastruttura descritto al punto successivo.
  - **Architettura Logica Hub&Spoke**: Per quanto riguarda l'ambiente Public cloud è previsto l'uso di un modello Hub & Spoke per consentire al PSN il controllo del traffico e la gestione delle DMZ per l'ambiente cloud. Le Amministrazioni potranno creare reti virtuali spoke nei segmenti, dove saranno attive Policy che forzeranno la connessione con Virtual Network Hub e impediranno la creazione di tipologie di risorse controllate centralmente, come, ad esempio, gli indirizzi IP pubblici.

- **Security & Governance:** l'architettura prevede la realizzazione di ambienti di erogazione di servizi presso i Data Center del PSN, che implementino servizi atti ad aumentare la sicurezza del Public Cloud, quali:



TIM - Uso Interno - Tutti i diritti riservati.

- servizi di **Key Management** tramite appliance HSM gestite, con l'obiettivo di sfruttare meccanismi di *Bring Your Own Key* (BYOK) sul Public Cloud, garantendo la proprietà e la completa gestione del ciclo di vita delle chiavi di cifratura in ambiente protetto e dedicato;
- servizi di **Backup** allo scopo di realizzare una seconda copia dei dati conservata all'interno del PSN e al di fuori del controllo del CSP, per assicurare in ogni momento il mantenimento della sovranità del dato;
- servizi professionali opzionali di gestione della sicurezza per monitorare continuamente le Security Posture dei Tenant su Public Cloud.

#### *2.9.2.2.1 Cifratura e gestione delle chiavi (Key Management)*

Vista la natura di sicurezza dei servizi del PSN, le capacità di crittografia della piattaforma sono fondamentali, in quanto non proteggono semplicemente il dato, ma, soprattutto, grazie al controllo all'accesso, sono il modo più efficace per esercitare il controllo sulla sovranità. È previsto che la piattaforma PSN fornisca servizi di crittografia e gestione delle chiavi e il servizio di *Key Management* deve essere basato su apparati HSM certificati FIPS 140-2 Level 3.
Di seguito la lista delle caratteristiche previste dall'architettura per il servizio:

- **Ambiente Public Cloud**:
  - È previsto l'uso dei servizi di gestione delle chiavi native, poiché questi sono integrati con la piattaforma. In questo modo i clienti saranno in grado di utilizzare un ampio spettro di servizi IaaS e PaaS mantenendo un forte controllo sull'accesso ai loro dati e alle loro chiavi. Per ottenere un controllo più stringente l'architettura prevede che ci sia la possibilità di gestire il ciclo di vita delle chiavi al di fuori del servizio di Key Management istanziato su Public Cloud (in particolare sarà possibile farlo con l'omologo servizio On-premise), e importare le chiavi all'interno del servizio Cloud, usando protocolli standard definiti allo scopo.

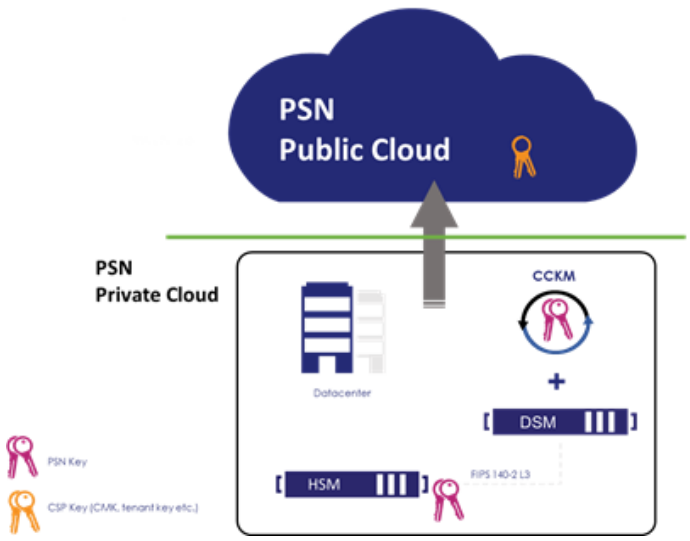



**Figura 7: Architettura Secure Cloud Service**

**L'architettura prevede che il servizio di Key Management sia implementato su Confidential Computing basandosi su apparati HSM FIPS 140-2 Level 3, con ulteriore livello di protezione per i dati in uso.**

- **Security Governance on-premise:**



TIM - Uso Interno - Tutti i diritti riservati.

- È necessario implementare un servizio di gestione delle chiavi poiché molte PA non hanno un HSM. La crittografia e la gestione delle chiavi fanno parte dei servizi di sicurezza di base richiesti dal PSN che deve fornire questo servizio.
- Il servizio deve consentire di gestire il ciclo di vita delle chiavi all'interno dei moduli di Key Management definiti all'interno dei *Tenant-Cloud* dei clienti.
- Per quel che riguarda il servizio di Key Management, l'architettura concettuale prevede la costruzione del servizio sfruttando software commerciali forniti da aziende specializzate nel settore, assicurandosi di implementare la corretta affidabilità del servizio stesso, essendo vitale per tutti gli ambienti che saranno definiti. La modalità di fruizione deve essere self-service, e deve essere garantita l'integrazione con i modelli e le interfacce di management previste, in modo da avere coerenza con il modello di gestione previsto dal disegno.
- La soluzione deve consentire le seguenti operazioni:
  - Generazione delle chiavi all'interno di apparati HSM;
  - Backup e restore delle chiavi;
  - Sincronizzazione delle chiavi con i servizi di Key Management del CSP;
  - Monitoraggio e auditing delle operazioni eseguite sulle chiavi;
  - Rotazione delle chiavi manuale e automatica;
  - Revoca della validità delle chiavi.

La crittografia è obbligatoria per tutte le applicazioni e i servizi ospitati nel PSN, mentre i servizi che devono implementare meccanismi di crittografia *at-rest* e/o *in-transit* e che devono integrarsi con il servizio di Key Management, sono quelli presenti nel catalogo servizi del Secure Public Cloud.

#### *2.9.2.2.2 Confidential Computing nell'ambito del PSN*

L'obiettivo del PSN è rafforzare il livello di confidenzialità e sicurezza del dato in uso tramite i seguenti metodi:

- ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations;
- usare tecniche di enforcement basate su componenti tecnologiche piuttosto che su processi organizzativi;
- fornire trasparenza sulle garanzie, i rischi residui e le mitigazioni che si possono implementare.

Il Confidential Computing va nella direzione di questi "driver" consentendo ai clienti di incrementare il controllo sul TCB in uso per l'esecuzione dei workload su ambiente Cloud, definendo con precisione tutto l'hardware e il software che ha accesso ai loro workload (dati e codice) e fornendo i meccanismi tecnici per applicare in modo verificabile questa garanzia (enforcement). In breve, è possibile mantenere il pieno controllo sui propri "*secrets*" rimuovendo il CSP dal Trusted Computing Base, riducendo così il confine di protezione solo all'hardware e all'applicazione stessa. Questa modalità consente a molti workload di poter essere utilizzati nel cloud pubblico, con un livello di protezione che si estende fino ad amministratori o utenti direttamente collegandoli all'hardware che esegue applicazioni. È quindi una tecnologia che



TIM - Uso Interno - Tutti i diritti riservati.

aumenta significativamente il grado di fiducia circa la capacità di proteggere la sovranità nel cloud pubblico, e questo lo rende particolarmente rilevante nell'architettura del PSN. Inoltre, grazie alla crescente integrazione delle funzionalità di Confidential Computing nei servizi PaaS, questo maggiore grado di fiducia può essere raggiunto con un impatto ridotto sulla capacità di innovazione fornita dai servizi Public Cloud. Questa combinazione di fattori rende il Confidential Computing una risposta molto efficace alle esigenze di Sovranità e Trasformazione Digitale del PSN.

Quindi i servizi di Confidential Computing consentono la rimozione del Cloud Service Provider dalla *Chain of Trust* a un livello senza precedenti rispetto al passato e offrono il più alto livello di sovranità disponibile oggi sul mercato nel cloud pubblico, migliorando sempre di più sotto questo aspetto. Ciò consente ai clienti e ai governi di soddisfare oggi le proprie esigenze di sovranità e di sfruttare l'innovazione domani.

L'architettura concettuale proposta prevede l'utilizzo del Confidential Computing sia nello scenario di migrazione Lift & Shift che negli scenari di nuove implementazioni o *renew/refactoring* di applicazioni esistenti, che vogliano abbracciare i paradigmi Cloud Native mantenendo un controllo stringente sull'accesso ai dati gestiti e al codice.

Per non compromettere la protezione offerta da questi servizi, occorre che lo stesso livello di controllo sia applicato a tutte le componenti dell'applicazione, in particolare al servizio di Key Management, ai servizi PaaS e/o di containerizzazione eventualmente usati e ai servizi di storage, che devono garantire l'encryption at rest del dato.

In conclusione, il Confidential Computing è una tecnologia all'avanguardia che consente un controllo su dati e risorse senza precedenti, i cui *security enforcement* non vanno a scapito dell'innovazione e della trasformazione digitale abilitate dai servizi cloud. E questa è una risposta solida agli obiettivi del PSN.

#### *2.9.2.2.3 Servizio di Backup*

Per la natura di sicurezza intrinseca del PSN, le capacità di governo dei dati della piattaforma sono fondamentali ed è evidente che, per esercitare la sovranità sullo stesso, sia altresì necessario garantire l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP. È per questo motivo che nel servizio Secure Public Cloud è prevista l'implementazione di un ulteriore livello di archiviazione all'interno dei Data Center del PSN per garantire la sovranità del dato. Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup-as-a-service presente nel Private Cloud del PSN in modo che lo Storage su cui risiede il dato protetto sia in completa gestione di personale del PSN. Questa integrazione prevede l'uso di tecniche di backup snapshot o stream-based e la cifratura dei dati "at rest" e in transito per garantire la protezione e ripristino delle macchine virtuali a cui è rivolto il servizio, anche di quelle che implementano meccanismi di encryption del disco di sistema e dei dischi dati. Infine, il servizio deve integrarsi con il modello di gestione previsto e consentire il controllo da parte del cliente finale.



TIM - Uso Interno - Tutti i diritti riservati.

#### 2.9.2.3 *Governance*

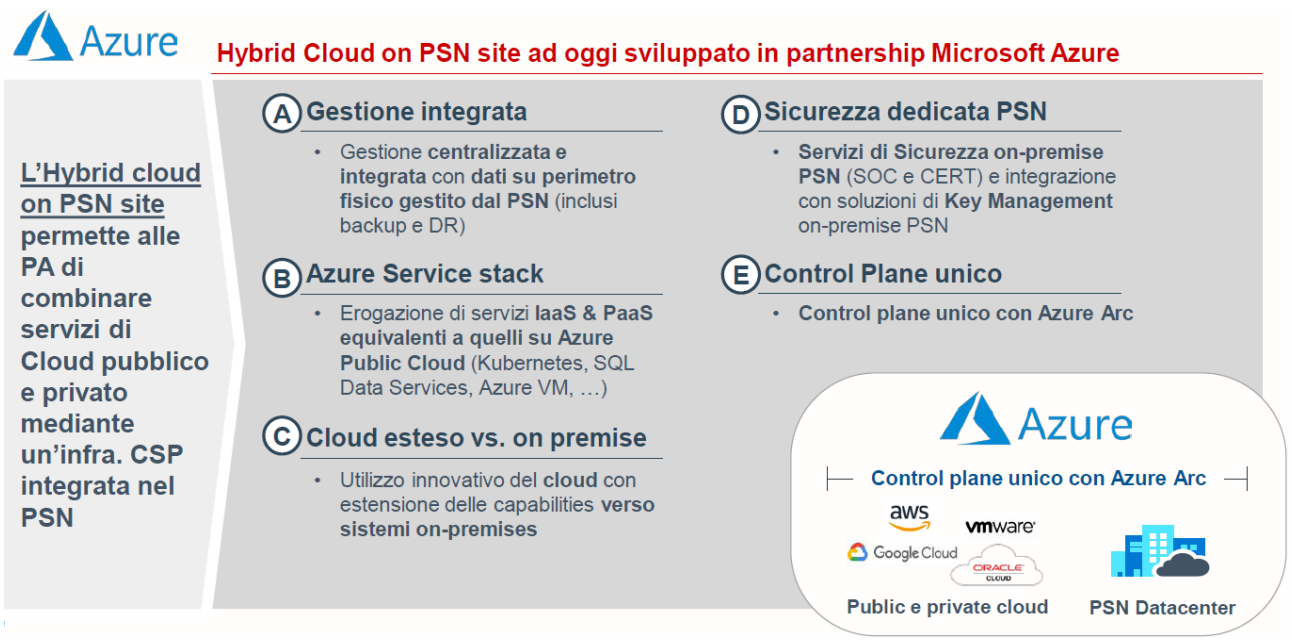
La gestione e la protezione degli account con privilegi amministrativi estesi è di fondamentale importanza per la consistenza del modello. Il disegno prevede che non siano presenti privilegi "persistenti" in nessuno degli ambienti connessi al PSN. Questo criterio si applica sia a tutti i repository di identità di tutti gli attori nonché a tutti i ruoli amministrativi degli ambienti di piattaforma realizzati in entrambi i lati dell'infrastruttura PSN. Il privilegio deve essere assegnato all'attore "candidato" ad assumerlo solo a valle di un processo autorizzativo, per un periodo limitato di tempo. Il processo di attribuzione del ruolo deve essere soggetto ad audit da parte del MSP-PSN e del cliente. Il processo può coinvolgere tutti gli attori sia per la fase autorizzativa (ad esempio cliente che autorizza il MSP ad assumere un ruolo, o responsabile del MSP che autorizza un operatore del MSP ad assumere un ruolo) che per la candidatura al ruolo (ad esempio operatore del MSP candidato al ruolo di contributor, o amministratore del cliente candidato al ruolo di Administrator). Tutti gli utenti che possono assumere ruoli con privilegi amministrativi devono usare meccanismi di autenticazione a più fattori.

Un altro meccanismo importante per l'implementazione del modello è il provisioning degli ambienti con l'applicazione automatica delle Policy, su entrambi i lati dell'infrastruttura del PSN. Questo garantisce che l'autonomia operativa dei clienti non deroghi dalle regole di sicurezza, pur lasciando libertà di implementare le proprie politiche di conduzione IT. Il MSP-PSN è responsabile della gestione del ciclo di vita delle Policy e della loro applicazione ai segmenti.

L'implementazione del servizio prevede la creazione dell'ambiente della PA e la realizzazione di un monitoraggio continuo per la garanzia della sicurezza del perimetro.

### 2.9.3 Hybrid Cloud on PSN Site

L'Hybridcloud on PSN site permetterà alle PA di combinare i servizi privati e ibridi dei CSP (Azure), su infrastruttura sicura PSN.

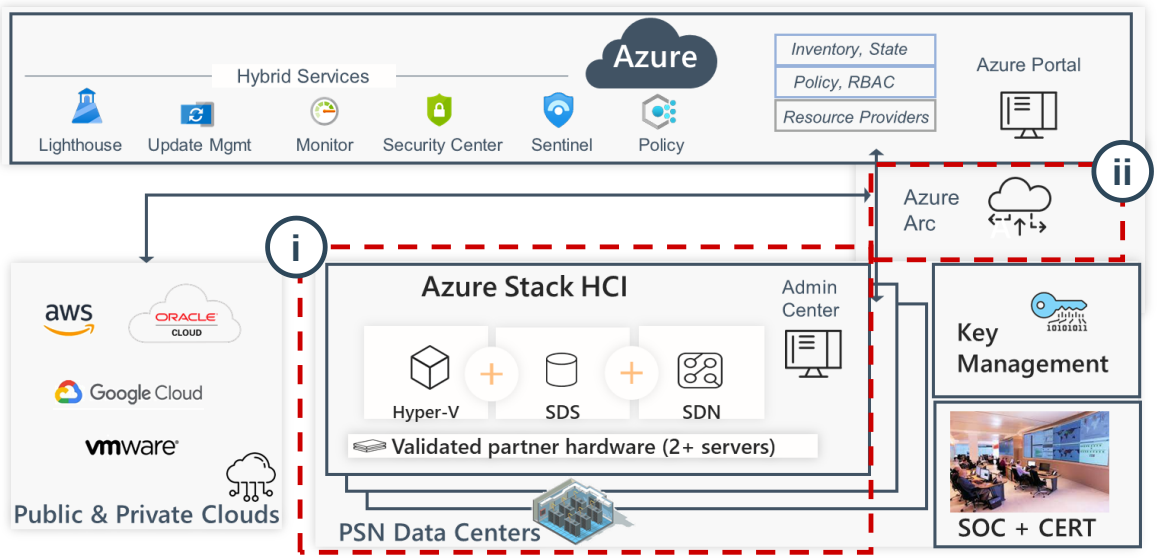





TIM - Uso Interno - Tutti i diritti riservati.

Il servizio mette a disposizione infrastrutture iperconvergenti dedicate:

I. basate su **soluzioni HCI** (Hyperconverged Infrastructure) **dedicate** a ciascun cliente e **ubicate all'interno** dei Data Center del **PSN**;
II. registrate nelle **subscription dei clienti,** che diventeranno «deployment target» utilizzabili attraverso il **control plane di Azure** (Portale, Powershell, CLI, Rest API, ...) per mezzo del servizio Azure Arc.;
III. caratterizzate da un **Management Plane** formato da**:**
   - una componente rimanente sull'**area On-premise** del servizio (Admin Center);
   - una componente che sfrutta i **servizi cloud Azure** per le funzionalità di monitoraggio, gestione aggiornamenti, raccolta eventi di sicurezza e controllo security posture.




Di seguito un focus sui servizi Azure stack HCI e Azure Arc:

I. **Azure stack HCI**
**Servizi di network altamente resilienti e consistenti grazie alle funzionalità della Software Defined Network:**
   - Infrastrutture implementate sul **paradigma SDDC** con a disposizione **servizi di virtualizzazione delle componenti di Compute, di Storage e di Network** e gestite:
     - **operativamente**, fino all livello Hypervisor, da **personale sistemistico;**
     - dal punto di **vista di sicurezza**, dal **SOC e CERT** del PSN.
   - Specifiche tecniche di un'**infrastruttura dedicata: variazione tra 2 e 16 nodi computazionali** basati su **server certificati** e **validati** per **ottimizzare le performance e la capacity** con:
     - processori di nuova generazione;
     - dimensioni adeguate al consolidamento dei workload;
     - storage Iperconvergente Ibrido (SSD/SAS);
     - infrastruttura di rete ad alte performance (25/40 Gbps).



TIM - Uso Interno - Tutti i diritti riservati.

II. **Azure Arc**

**Gestione uniforme ed omogenea dell'infrastruttura *iperconvergente* che garantisce flessibilità in compute e storage:**

- **Distribuzione servizi Cloud Native di tipo Paas** *(Orchestrazione di container – Kubernetes; DB-as-a-service - SQL & PostgreSQL; Web App Services - FaaS, Logic App; Machine learning & AI Service; Virtual Desktop-as-a-service).*
- **Gestione da parte dei clienti del ciclo di vita delle virtual machine** su Azure Stack HCI attraverso il portale Azure (come previsto per il servizio Secure Public Cloud o altri servizi su Azure).
- Definizione sulla base di Azure Policy di un **set di policy di sicurezza e di monitoraggio,** che verranno propagate e applicate a tutti i workload integrati tramite Azure Arc in tutti gli ambienti disponibili a partire dal Hybrid Cloud on PSN Site fino ad altri Hyperscaler o ambienti on-premise cliente.

L'architettura concettuale propone una soluzione di tipo "Hybrid Cloud" basata su due componenti principali:

- Un servizio di tipo **Hyperscale Public Cloud** erogato da una *Region* collocata sul territorio nazionale, per la sola erogazione di un **control plane** unificato;

- Un servizio erogato dai Data Center del PSN distribuiti sul territorio Nazionale di tipo "**PSN Private Cloud**" che fornirà le risorse infrastrutturali e le componenti di servizio erogate verso le PA.

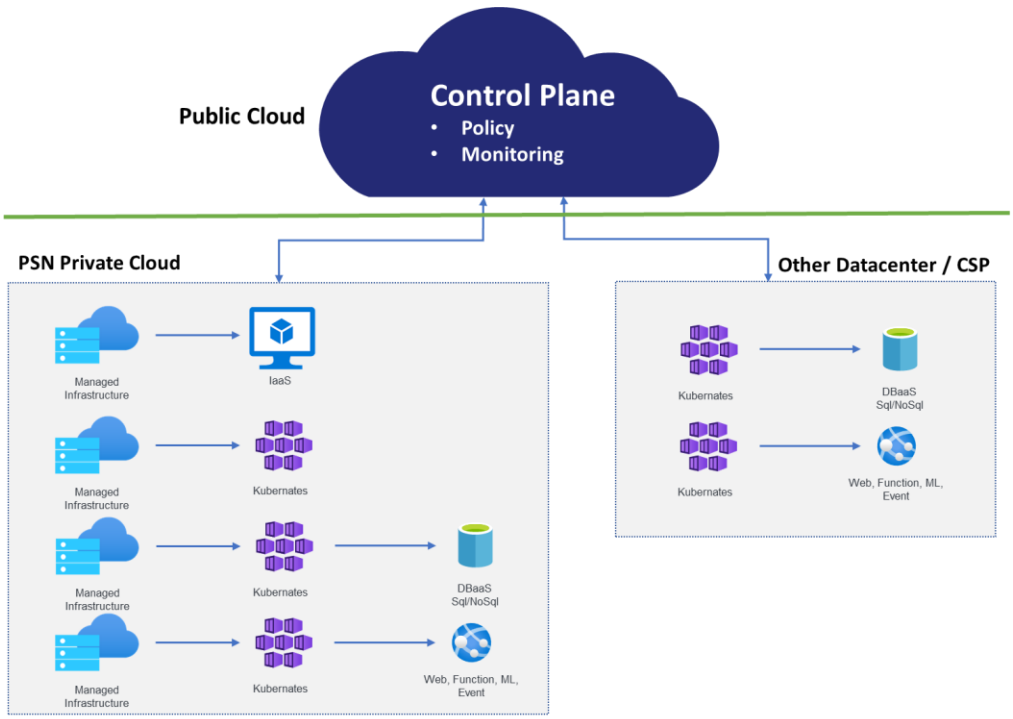



**Figura 8: Control Plane e architettura servizio**



TIM - Uso Interno - Tutti i diritti riservati.

Il modello di governance prevede l'estensione verso la componente Hosted-On-PSN Private Cloud del modello implementato in ambito Public Cloud grazie a tecnologie che consentono di usare il control plane del Public Cloud anche per governare la componente on-premise o su altri data center.

Il PSN avrà responsabilità di gestione e manutenzione delle componenti hardware e software presenti on-premise che nel modello public cloud sono delegate al CSP.

Ad ogni cliente che aderisce al servizio verrà messa a disposizione una **infrastruttura fisica dedicata** basata su un cluster di server modulare che potrà crescere/decrescere con la granularità del singolo server.

Su questa infrastruttura dedicata (denominata Tenant-On-prem) sarà possibile governare la creazione e gestione di servizi in modalità IaaS e PaaS sfruttando template messi a disposizione ad-hoc, gestiti e aggiornati tramite il control plane unificato su Public Cloud. Inoltre, la gestione della Capacity del cluster fisico dedicato e della relativa variazione delle risorse hardware in uso andrà gestita tramite Service Request che il cliente inserirà su sistema di ITSM dal PSN e che verranno indirizzate tramite opportuni interventi operativi.

La disponibilità di servizi PaaS in ambienti on-premise dovrà essere basata su implementazioni su cluster Kubernetes. In questo scenario, la gestione di questo cluster e delle risorse assegnate ai servizi PaaS rimane in carico al cliente ed avviene in coerenza con il modello di gestione.

L'architettura PSN non prevede livelli di astrazione, come ad esempio portali o strumenti sviluppati ad hoc per la gestione e il controllo degli ambienti, ma, al contrario, fornisce nativamente un'esperienza coerente sia per AppOps (gestito dal cliente stesso) che per DevOps (team operativi applicativi dedicati). Non prevede inoltre una distinzione di gestione e di ambienti tra vecchie e nuove applicazioni o fra adozione di paradigmi IaaS e PaaS. In definitiva, l'architettura consente la predisposizione di ambienti sicuri per tutte le infrastrutture e applicazioni da distribuire sulla piattaforma PSN. Per raggiungere tale obiettivo, qualsiasi sia l'interfaccia utilizzata, il Control Plane e il Management Plane rendono disponibile un modello unico e coerente di gestione di tutte le risorse PSN e dei canali di provisioning/deprovisioning, soggetto a controlli basati sui ruoli (RBAC) e Policy. Quindi tutti gli attori, in base ai loro ruoli e responsabilità, avranno la possibilità di utilizzare lo stesso Control/Management Plane per stabilire un insieme standardizzato di Policy e controlli per governare l'intero patrimonio IT definito nel PSN.

La gestione dell'utente e dei diritti ad esso assegnati permette la segregazione degli stessi in ciascun ambito senza propagazione automatica di diritti tra il mondo Distributed Cloud e quello PSN. Questo sistema flessibile e granulare permette di mantenere le identità ove il ciclo di vita delle stesse garantisce la massima accuratezza, con possibilità di avere set di diritti diversi nei vari contesti e completo controllo dell'attivazione dei privilegi quando necessario. Il sistema di controllo centralizzato permette reportistica accurata e coerente degli accessi e delle assegnazioni dei privilegi nonché delle azioni effettuate sulle risorse target.

L'architettura dell'Hybrid Cloud on PSN on Site deve essere in grado di garantire alti livelli di affidabilità tramite implementazione di soluzioni di astrazione delle risorse fisiche (es. soluzioni



TIM - Uso Interno - Tutti i diritti riservati.

SDDC) che permettano di gestire infrastrutture di elaborazione sottostanti distribuite su diversi data center collegati tra loro a bassa latenza.

L'Hybrid Cloud on PSN on Site fornirà i seguenti servizi:

- IaaS: Creazione e gestione di VM e del logical networking;
- Container as a Services implementato su diverse distribuzioni;
- DBaaS: Servizi di DBaaS basati su software commerciali e open source, quali:
  - PostgreSQL;
  - MySQL;
  - Microsoft SQL DB/SQL Managed Instances;
- PaaS per servizi per l'implementazione di applicazioni ServerLess, quali:
  - Web Application;
  - Function as a Service;
  - Integration services;
  - Eventing as a service;
- NoSQL DBaaS;
- Machine Learning as a service.

Infine, sfruttando le tecnologie di gestione di ambienti Distributed Cloud che proiettano sul control plane del Public Cloud le risorse definite su altri ambienti, siano essi altri Data Center on premise o altri cloud provider, è possibile estendere il modello di gestione anche verso questi altri ambienti, abilitando lo scenario ibrido e multicloud e mantenendo coerenza di automazione, sicurezza, governance e gestione.

## 2.10 Multi Cloud

A completamento dell'offerta dei servizi Cloud proposti nel presente progetto, la NewCo PSN offre la possibilità di integrarsi con le migliori soluzioni di Public Cloud dei principali player e Cloud Provider internazionali. L'offerta Multicloud si propone come soluzione completa di architetture Hybrid & Multicloud e come interfaccia unica verso il cliente, indipendentemente dal cloud provider di riferimento. Il PSN è in grado di disegnare architetture su misura proponendo al cliente soluzioni basate sulle proprie offerte e sul best-in-class dei Public Cloud Provider, armonizzando e ottimizzando le specifiche logiche per sfruttare al massimo le caratteristiche dei singoli cloud, dei nuovi servizi e delle nuove tecnologie.

### 2.10.1 Cloud Management Platform



TIM - Uso Interno - Tutti i diritti riservati.

La Console Unica descritta nel documento "*Specificazione delle caratteristiche del servizio*", resa disponibile a tutte le Amministrazioni che contrattualizzeranno servizi proposti nel presente progetto, è applicabile anche in un contesto Multicloud e si integra con le funzionalità della Cloud Management Platform, unico punto di gestione per i servizi standard erogati dal PSN. Attraverso servizi professionali (opzionali) è possibile estendere le capabilities standard con funzionalità aggiuntive o personalizzazione.

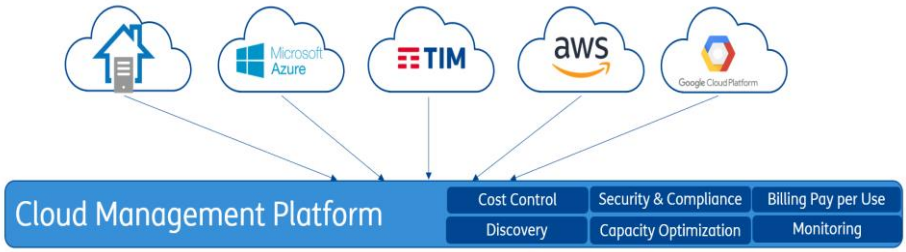



**Figura 9: Cloud Management Platform**

Pertanto, la Console Unica di Gestione permetterà alle amministrazioni aderenti di gestire i servizi sul PSN e su altri Cloud Service Provider, attraverso le funzionalità riassunte di seguito:

- Portale self-service con catalogo dei servizi unificato;
- Servizi di infrastruttura (designing, provisioning e management di infrastrutture multi-cloud);
- Interazione via API per modelli Cloud Agnostic di IaC (con integrazione Git repositories e strumenti di CI/CD);
- Servizi e BluePrint tecnologiche;
- Dashboard di Performance Monitoring, analisi predittiva e definizione di allarmi per superamento soglie;
- Interfaccia interattiva di misurazione e gestione dei consumi e delle risorse;
- Strumento di costruzione di report di Cost Control e Resource Usage;
- Gestione finanziaria dell'IT.

Sono inoltre disponibili come servizi aggiuntivi (che richiedono in ogni caso attività professionali di configurazione e implementazione su CU e CMP) funzionalità di:

- Governance (diritti di utilizzo, approvazioni, recupero, showback);
- Servizi e BluePrint tecnologiche personalizzati;
- Workflow personalizzati;
- Capacity Planning Avanzato (corretto dimensionamento, modellazione, scenari di tipo "what-if" e funzionalità analitiche basate su modelli di capacità);
- Advanced Monitoring (può richiedere l'installazione di componenti sui server del cliente);
- Security, Compliance & Remediation in ambito MultiCloud (vedi sotto).



TIM - Uso Interno - Tutti i diritti riservati.

### 2.10.2 Security & Compliance in ambito Multi Cloud

Con la natura dinamica delle applicazioni multi-cloud, è essenziale effettuare frequentemente le operazioni mirate a mantenere la sicurezza e la conformità dei Servizi e delle applicazioni. La piattaforma CMP, opportunamente configurata e personalizzata per le specifiche esigenze delle singole Amministrazioni può automatizzare i test e la correzione della configurazione delle risorse cloud, in modo che i servizi cloud non contengano vulnerabilità dipendenti dalle configurazioni stesse. I controlli di sicurezza effettuati dal software sono basati su policy (ad es.: GDPR, CIS, PCI, Custom) e valutano automaticamente le configurazioni di risorse cloud e container rispetto alle migliori best practices. La funzionalità attivabile di remediation automatica colma rapidamente le lacune e facilita la gestione nel cloud, in AWS, Azure e Google Cloud.

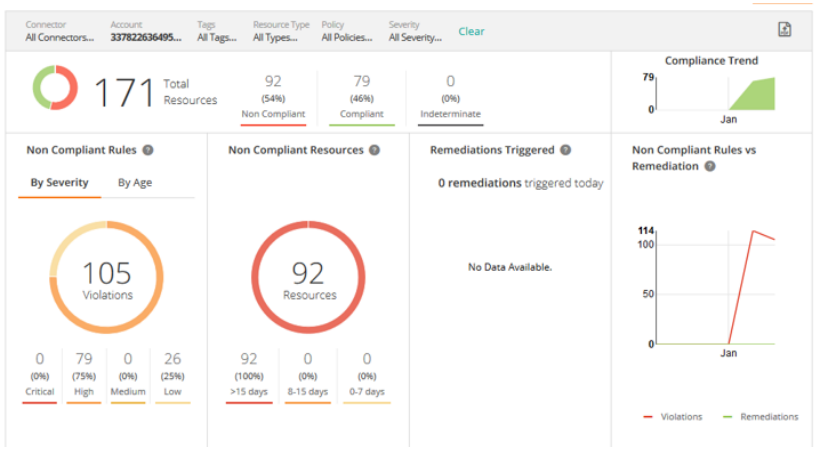



**Figura 10: Esempio dashboard Sec&Compliance**

## 2.11 Servizio di Migrazione, Evoluzione e Professional Services

In base al Piano di Digitalizzazione 2020-2022 le PA che utilizzano CED che non soddisfano i parametri definiti nella circolare AgID n. 01 del 14 giugno 2019 non possono fare investimenti di espansione ma dovranno, essere migrati nel Private Cloud della NewCo PSN. A valle della richiesta di poter usufruire dei servizi offerti dalla NewCo PSN, le PA forniranno l'elenco aggiornato del perimetro IT e TLC coinvolto nell'affidamento del servizio, con indicazione delle modalità richieste (Housing, Hosting, IaaS). Tale elenco fornirà gli elementi per poter identificare l'insieme dei Servizi e relative modalità di fruizione e contrattualizzare il rapporto tra la NewCo PSN e le PA.

### 2.11.1 Figure Professionali

La NewCo PSN renderà disponibili risorse professionali in grado di poter supportare le Amministrazioni in tutte le attività/necessità che si renderanno necessarie nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-host, re-architect, re-platform), proseguendo nella fase di riavvio degli applicativi, regression test e terminando nel supporto all'esercizio.

Per ogni progetto verrà individuata il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste. Il team mix potrà esser composto da una o più delle seguenti figure professionali:

a) **Project Manager:** definisce e gestisce i progetti, adottando e promuovendo metodologie agili; è responsabile del raggiungimento dei risultati, conformi agli standard di qualità,



TIM - Uso Interno - Tutti i diritti riservati.

sicurezza e sostenibilità, in coerenza con gli obiettivi, le performance, i costi ed i tempi definiti.

b) **Enterprise Architect**: ha elevate conoscenze su differenti aree tecnologiche che gli permettono di progettare architetture enterprise, sviluppando modelli basati su Enterprise Framework; è responsabile di definire la strategia abilitante per l'evoluzione dell'architettura, mettendo in relazione la missione di business, i processi e l'infrastruttura necessaria.

c) **Cloud Application Architect**: ha conoscenze approfondite ed esperienze progettuali nella definizione di architetture complesse e di Ingegneria del Software dei sistemi Cloud ed agisce come team leader degli sviluppatori ed esperti tecnici; è responsabile della progettazione dell'architettura di soluzione applicative di cloud computing, assicurando che le procedure e i modelli di sviluppo siano aggiornati e conformi agli standard e alle linee guida applicabili

d) **Cloud Application Specialist**: ha consolidate conoscenze tecnologiche delle soluzioni cloud e dell'integrazione di soluzioni applicative basate su un approccio cloud computing based; è responsabile della delivery di progetti basate su soluzioni Cloud.

e) **Business Analyst**: È responsabile dell'analisi dei dati anche in ottica di business, e della relativa raccolta dei requisiti necessari a migliorare la qualità complessiva dei servizi IT forniti.

f) **Cloud Security Specialist**: esperto nella progettazione di architetture di sicurezza per sistemi basati su cloud (public ed hybrid). È responsabile per il supporto alla realizzazione delle architetture di sicurezza dei nuovi workload delle Amministrazioni e alle attività di migrazione, fornisce indicazioni e raccomandazioni strategiche ai team operativi e di sviluppo per affrontare i punti deboli della sicurezza e identificare potenziali nuove soluzioni di sicurezza negli ambienti cloud

g) **Database Specialist and Administrator:** È responsabile dell'installazione, dell'aggiornamento, della migrazione e della manutenzione del DBMS; si occupa di strutturare e regolamentare l'accesso ai DB, monitorarne l'utilizzo, ottimizzarne le prestazioni e progettare strategie di backup

h) **Devops Expert**: Ha consolidata esperienza nelle metodologie di sviluppo DevOps su progetti complessi, per applicare un approccio interfunzionale in grado di garantire la sinergia tra i team di sviluppo e di gestione dei sistemi; è responsabile di progettare le strategie DevOps, identificando gli strumenti di controllo dei sorgenti, di automazione e di rilascio in ottica Continuous Integration e Continuous Development.

i) **System and Network Administrator**: ha competenze sui sistemi operativi, framework di containerizzazione, tecnologie di virtualizzazione, orchestratori e sistemi di configuration e versioning; è responsabile della implementazione di sistemi di virtualizzazione, di container utilizzando anche sistemi di orchestrazione e della manutenzione, della configurazione e del funzionamento dei sistemi informatici di base.

j) **Developer (Cloud/Mobile/Front-End Developer)**: Ha competenze di linguaggi di programmazione e di piattaforme di sviluppo, utilizzando le conoscenze di metodologie di analisi e disegno OOA, SOA e REST con UML; assicura la realizzazione e l'implementazione di applicazioni con architetture web-based e cloud-based.



TIM - Uso Interno - Tutti i diritti riservati.

k) **UX Designer**: ha una conoscenza teorica e pratica dei principi di usabilità, paradigmi di interazione e principi di interaction design e di gestione delle problematiche di compatibilità cross-browser (desktop, tablet, mobile); è responsabile dell'applicazione dell'approccio centrato sull'utente (human centered) nello sviluppo dei servizi digitali, garantendo il raggiungimento efficace ed efficiente degli obiettivi dell'utente nell'interazione con l'Amministrazione.

l) **System Architect:** ha consolidata esperienza in technical/service management e project management, analizza i sistemi esistenti e definisce come devono essere coerentemente integrate le nuove soluzioni; è responsabile della progettazione della soluzione infrastrutturale e del coordinamento di specifici stream di progetto

m) **Product/Network/Technical Specialist**: È responsabile delle attività inerenti all'integrazione delle soluzioni tecniche ed il supporto specialistico di prodotto nell'ambito dell'intervento progettuale.

n) **Security Principal**: Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.

o) **Senior Information Security Consultant**: Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.

p) **Junior Information Security Consultant**: Garantisce l'esecuzione delle misure di sicurezza per proteggere le reti ed i sistemi informatici. Attua le regole definite in materia di sicurezza delle informazioni.

q) **Senior Security Auditor/Analyst**: Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia. Completa i giornali di audit documentando test e risultati dell'audit.

r) **Security Solution Architect**: Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.

s) **Data Protection Specialist**: Figura professionale dedicata ad affiancare il titolare, gli addetti ed i responsabili del trattamento dei dati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo.



TIM - Uso Interno - Tutti i diritti riservati.

t) **Junior Security Analyst**: Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.

u) **Forensic Expert**: E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

v) **Senior Penetration Tester**: Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.

w) **Junior Penetration Tester**: Effettua tentativi di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza in accordo con quanto definito le progetto di riferimento.

x) **System Integration & Test Specialist**: Contribuisce in differenti aree dello sviluppo del sistema, effettuando il testing delle funzionalità del sistema, identificando le anomalie e diagnosticandone le possibili cause. Utilizza e promuove strumenti automatici.

y) **Educational Designer/Tutoring:** Struttura, organizza e schedula i programmi di formazione, ne valuta la qualità attraverso un processo di feedback.

### 2.11.2 Migrazione

I servizi di Migrazione saranno quantificati e valutati economicamente sulla base di specifici assessment da condurre in fase di definizione delle esigenze dell'Amministrazione tenendo conto di eventuali vincoli temporali ed architetturali di dettaglio oltre che di specifiche esigenze di customizzazione.

Per l'intero periodo, la NewCo PSN metterà a disposizione delle PA le seguenti figure professionali:

1. Un **Project Manager,** che dovrà coordinare le attività e che dovrà collaborare col referente che ogni singola PA dovrà indicare e mettere a disposizione;
2. Un **Technical Team Leader** che seguirà tutte le fasi più strettamente legate agli aspetti operativi.

Si chiederà alla PA la disponibilità di fornire uno o più referenti coi quali il Project Manager e il Technical Team Leader della NewCo PSN si possano interfacciare.

Verranno inoltre condivisi:

- la lista dei deliverables di Progetto;
- la Matrice di Responsabilità;
- gli exit criteria di ogni fase di progetto;
- il Modello di comunicazione tra NewCo PSN e PA.



TIM - Uso Interno - Tutti i diritti riservati.

A seguito dell'invio del Piano dei Fabbisogni da parte dell'Amministrazione – non descritto nel presente Progetto di fattibilità:

1) verrà indetto, da parte della NewCo PSN, il Kick off di Progetto tra la NewCo PSN e la PA durante il quale verranno identificati gli stakeholders di Progetto della NewCo PSN e della PA.

2) Entro 60 giorni successivi al Kick off di Progetto, la NewCo PSN, avvalendosi del supporto del/dei referenti delle PA, comunicati in sede di Kick off, presenterà il documento "**Progetto del Piano dei Fabbisogni**", contenente il "**Piano di Migrazione di Massima"** dove verranno definite le macro-attività di progetto. La PA, una volta ricevuto il suddetto Progetto del Piano dei Fabbisogni, potrà, entro i successivi 10 giorni, approvarlo, ovvero far pervenire alla NewCo PSN le proprie osservazioni che dovranno essere recepite dalla NewCo PSN entro i successivi 10 giorni lavorativi.

   Ogni Piano di Migrazione sarà articolato secondo i seguenti capitoli descriventi le 4 fasi di Progetto 1) Analisi, 2) Setup, 3) Migrazione, 4) Collaudo.

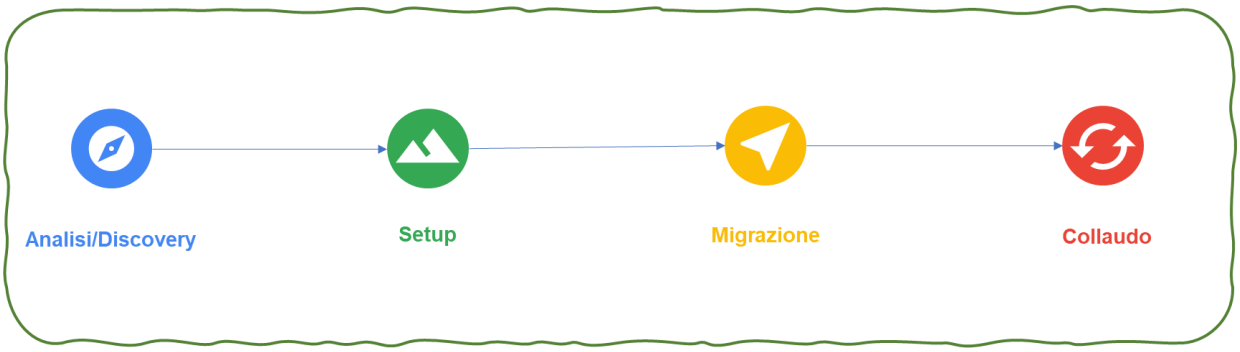



**Figura 11: Flusso di Migrazione**

**I. Analisi/Discovery**

a) delle piattaforme oggetto della migrazione;
b) delle applicazioni erogate dalla PA
c) dei dati oggetto di migrazione;
d) degli SLA delle singole applicazioni;
e) di eventuali finestre utili per la migrazione;
f) di eventuali periodi di indisponibilità delle applicazioni;
g) del Cloud Maturity Model;
h) analisi della sicurezza dell'ambiente da migrare;
i) Energy Optimization.

Al fine di supportare le PA nel processo di adozione del Cloud è necessario identificare un modello per la valutazione oggettiva del livello attuale dell'ente da analizzare e degli interventi di adeguamento necessari. Il modello di riferimento che intendiamo proporre è il Cloud Maturity Model, modello standard che ha lo scopo di definire un approccio strutturato e una serie di controlli



TIM - Uso Interno - Tutti i diritti riservati.

da attuare per valutare il cosiddetto «livello di maturità» attuale del Cloud della PA ed i gap rispetto al livello atteso, al fine di rispettare gli obiettivi del PNRR. L'approccio proposto supporta pienamente e completa le indicazioni di AgID per implementare il processo di evoluzione verso il cloud.

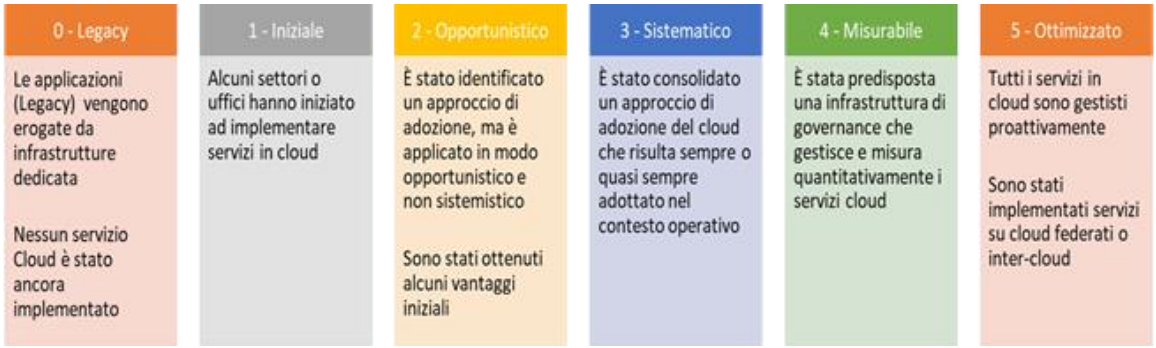



**Figura 12: Cloud Maturity Model**

Più specificatamente, al fine di valutare correttamente ed efficacemente il livello di maturità si procederà con un assessment. I controlli valuteranno differenti aspetti afferenti a domini tecnici e non tecnici, attraverso la predisposizione di benchmark e di questionari che verranno compilati con il supporto della PA. Al termine di ogni controllo saranno individuati i gap da colmare per portare il livello complessivo di adozione dal valore attuale (current level) fino al valore atteso (target level). La Figura 13 presenta un esempio del livello attuale (in azzurro) e target (in ocra), sui ciascuno dei diversi domini di valutazione individuati.

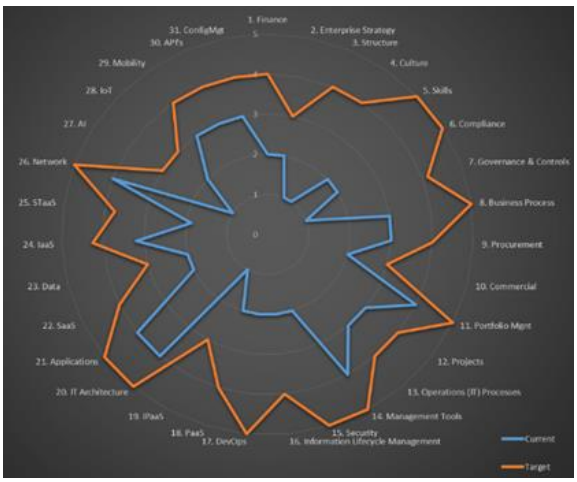



**Figura 13: Livelli attuali e target del Cloud Capability Maturity Model**

Un approccio basato sulla valutazione del livello di maturità di adozione prevede quindi:

i) l'applicazione del modello per valutare il livello di maturità oggettivo (current) dell'adozione cloud;

ii) la valutazione del gap rispetto al livello atteso;

iii) l'individuazione di interventi focalizzati per migliorare il livello di adozione e raggiungere il livello atteso;



TIM - Uso Interno - Tutti i diritti riservati.

iv) la pianificazione e l'implementazione degli interventi individuati;

v) la verifica ex-post con nuova valutazione del livello di adozione per verificare l'efficacia degli interventi di miglioramento attuati.

Nella fase di Analisi/Discovery sarà anche valutata l'attuale postura in termini di sicurezza applicativa e infrastrutturale attraverso l'uso di analisi DAST e VA effettuati verso le applicazioni esistenti nella PA richiedente.

Inoltre, la **Discovery** ha lo scopo di raccogliere tutte le informazioni relative alla infrastruttura e ai workload da migrare. Questa attività consente di comporre un inventory ed una check list che supporteranno le successive attività e permetteranno, in fase di collaudo, la verifica di tutte le componenti, hardware e software migrate. Al termine dell'attività di discovery verrà prodotto un registro della configurazione delle componenti da migrare condiviso e sottoscritto dall'Amministrazione. Le successive fasi della migrazione dovranno stabilire verso quale tipo di infrastruttura, d'accordo con il/i referenti delle PA, sarà indirizzata. Eventuali cambiamenti che si rendessero necessari durante la migrazione, dovranno essere riportati nel registro stesso.

Di seguito si riporta un esempio di possibile registro della configurazione

| Componente | Descrizione | Versione/ Modello | Licenza e Manutenzione | Documentazione | Note |
|---|---|---|---|---|---|
| S.O. server XYZ | Sistema operativo installato sul server fisico XYZ | Windows Server 2012 | Sì, sottoscrizione annuale | Disponibile al link ... | Server per il servizio di cartelle condivise |

Al fine di migliorare la sostenibilità energetica della digitalizzazione della PA, verrà erogato un servizio di Energy Optimization atto a valutare ed ottimizzare i consumi energetici dell'infrastruttura e dei workload da migrare. Questo tipo di servizio si basa sull'insieme di tecniche e competenze che vanno sotto il nome di "green computing".

Per quanto riguarda la valutazione, questa verrà fatta assumendo come valore di riferimento il consumo (misurato o stimato sulla base dei valori di targa) dell'infrastruttura prima che questa venga migrata. Seguirà una valutazione circa l'utilizzo delle risorse HW e SW da impegnare nel PSN con il preciso scopo di contenere i consumi, ad esempio valutare la frequenza del processore, la dimensione della memora volatile e di massa, il tipo stesso di processore, etc...

A seguito della migrazione si propone poi una fase di ottimizzazione energetica del workload e dell'hardware, basata su misure di consumo fatte direttamente nelle infrastrutture del PSN.
L'output del processo di ottimizzazione può includere prescrizioni, come ad esempio l'aggiornamento della versione del software al fine di meglio sfruttare le caratteristiche dell'HW, oppure suggerimenti sull'utilizzo degli applicativi.

La scelta della strategia di migrazione sarà effettuata tra quelle indicate nel documento "manuale di abilitazione al cloud" di AgID e note come le 6R (Retain, Retire, Re-purchase, Re-host, Re-platform e Re-architect) e avverrà sulla base delle risultanze dell'analisi dell'ambiente e delle esigenze espresse dalla singola PA. Ad eccezione dei casi di Housing, la migrazione sarà effettuata



TIM - Uso Interno - Tutti i diritti riservati.

principalmente in modalità Re-Host (lift&Shift) che consiste nel "prendere" (Lift) l'intero servizio, compreso di infrastruttura, architettura, dati e traffico e "spostarlo" su un hosting cloud (Shift) senza modifiche al core dell'applicativo. La migrazione potrà esser effettuata in due modalità manuale e automatizzata. Questa strategia permette di effettuare un primo passo verso il cloud lasciando aperta la possibilità, successivamente, di implementare ulteriori miglioramenti all'applicativo che consentano di sfruttare ulteriormente i vantaggi del cloud andando ad utilizzare altre strategie di migrazione previste dal paradigma delle 6R, ossia Re-Platform e Re-Architect.

II. **Setup**
   a) predisposizione dell'infrastruttura target presso i nuovi DC:
      (1) Disegno dei workload;
      (2) Definizione architettura logica e fisica;
      (3) Configurazione ambienti;
   b) se richiesto, come servizio aggiuntivo, predisposizione dell'infrastruttura di networking relativa alla connessione tra la PA e i nuovi DC.

III. **Migrazione**
   a) Trasferimento dei dati;
   b) Implementazione policy di sicurezza;
   c) Impostazione del monitoraggio.

IV. **Collaudo**
   a) Finalizzato a testare le procedure e modalità della migrazione. A seguito del collaudo funzionale della intera infrastruttura di ogni PA, la NewCo PSN dovrà prevedere l'attivazione di tutti i Servizi richiesti dalla PA (riferimento §. 2.3.5 Collaudi e verifiche di conformità del documento "*Specificazione delle caratteristiche del servizio e della gestione*").

Tutte le fasi di migrazione verranno eseguite tenendo conto di:

a) Valutazione dei Rischi;
b) Conduzione di Misure Specifiche di Valutazione del Rischio e Esecuzione di Test Preliminari;
c) Definizione delle Strategie di Mitigazione e delle Contromisure;
d) Definizione dei metodi di Monitoraggio del Rischio e dei Punti di Controllo (checkpoint) durante la Trasformazione;
e) Monitoraggio continuo del Rischio durante tutte le fasi di progetto.

3) Entro **60 giorni** dall'approvazione da parte della PA del Progetto del Piano di Fabbisogni, contenente il Piano di Migrazione di Massima, la NewCo PSN, avvalendosi del supporto del/dei referenti delle PA, comunicati in sede di Kick off, definirà e consegnerà alla PA il "**Piano di Migrazione di Dettaglio"** contenente le tempistiche e il dettaglio delle modalità operative di quanto contenuto nel Piano di Migrazione di Massima.
   Nello specifico, Il "Piano di Migrazione di Dettaglio" dovrà evidenziare gli aspetti logistici, infrastrutturale, organizzativi e procedurali previsti per l'erogazione di quanto contenuto nel



TIM - Uso Interno - Tutti i diritti riservati.

Piano di Migrazione di Massima, nonché la pianificazione temporale con cui verranno effettuate le attività.
La PA, una volta ricevuto il suddetto "**Piano di Migrazione di Dettaglio"**, potrà, entro i successivi 10 giorni approvarlo, ovvero far pervenire alla NewCo PSN le proprie osservazioni che dovranno essere recepite dalla NewCo PSN entro i successivi 10 giorni lavorativi.

### 2.11.3 Servizi di Evoluzione

La NewCo PSN renderà disponibili alle Amministrazioni servizi di evoluzione con l'obiettivo di: ✓migliorare eventuali ambienti precedentemente migrati sulla piattaforma PSN tramite Re-Host o tramite i servizi di Housing/Hosting; ✓ supportare la migrazione di applicativi on premise verso una piattaforma cloud tecnologicamente avanzata, in modo da beneficiare delle funzionalità messe a disposizione dall'infrastruttura proposta, come sicurezza, scalabilità e ottimizzazione di costi e risorse.

In particolare, i due servizi forniti, afferenti alle 6R delle strategie di migrazione al cloud, saranno quelli di Re-platform e Re-architect, in quanto queste due strategie di migrazione sono quelle che maggiormente massimizzano i benefici per l'Amministrazione di una piattaforma cloud come quella oggetto del presente progetto.

I due servizi si differenziano principalmente per la quantità del codice applicativo che viene modificato e, di conseguenza, per le tempistiche di attuazione. Il Re-platform modifica solamente alcuni componenti senza impattare il core dell'applicativo, mentre il Re-architect permette di portare l'applicazione in Cloud attraverso interventi puntuali sulla stessa.
Tali servizi non sono necessariamente alternativi ma possono eventualmente rappresentare fasi sequenziali di un programma di modernizzazione applicativa.
Per questi servizi, in base alla specifica esigenza, verrà proposto un **team mix** composto dai profili professionali sopra elencati.

#### 2.11.3.1 *Re-platform*

La strategia di Re-platform oltre a trasferire un applicativo sul cloud come avviene nel re-host, sostituisce nel processo di migrazione alcune componenti per meglio sfruttare le specificità della piattaforma di destinazione. La finalità principale della strategia è di trasferire l'applicativo in cloud senza stravolgimenti funzionali, analizzando i possibili interventi che consentono di cogliere, rispetto ai benefici garantiti da una soluzione cloud-native, il livello massimo di ottimizzazione e beneficio. Gli interventi si concentrano sul cambio di SO/DB, Software Update, DB Update con l'obiettivo di standardizzare le componenti infrastrutturali e permetterne una più semplice gestione di configurazione. Il servizio può rendersi necessario qualora il livello di sicurezza non sia conforme allo standard minimo; pertanto realizza la modifica di componenti specifici di un'applicazione verso sistemi IaaS e PaaS erogati dal PSN al fine di migliorarne la scalabilità ma soprattutto la sicurezza.

Di seguito vengono illustrati i diversi step del processo di Re-platform:



TIM - Uso Interno - Tutti i diritti riservati.

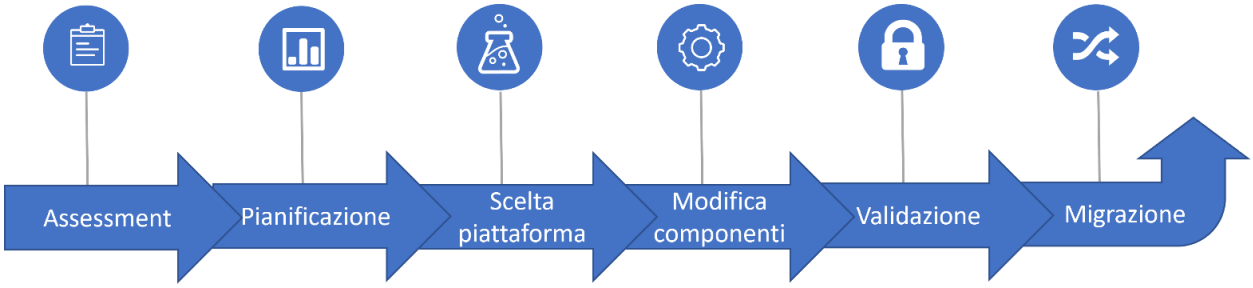



**Figura 14: Flusso processo di Re-platform**

Nella fase di *Assessment* viene condotta un'analisi dell'applicazione per comprenderne le caratteristiche e poter valutare se la strategia di Re-platform sia adatta allo scopo, definendo le componenti dell'applicazione che possono essere sostituite.

In particolare, alcune delle caratteristiche che vengono analizzate sono:

- architetture modulari e a componenti separabili a diversi livelli di granularità;
- uso di componenti sostituibili con l'equivalente servizio cloud-native;
- eventuali dipendenze dall'hardware fisico;
- disponibilità e modificabilità del codice sorgente;
- criticità legate a componenti sostituibili con un'alternativa cloud native;
- disponibilità di documentazione tecnica che supporti nella sostituzione delle componenti.

Dopo l'Assessment dell'applicativo, segue una fase di *Pianificazione* della migrazione ed una successiva *Scelta della piattaforma* cloud tra quelle disponibili nel catalogo. Successivamente vengono *Modificati i componenti* con quelli individuati in fase di assessment, viene validata la soluzione e infine l'applicazione viene *Migrata* sulla piattaforma PSN.

I vantaggi offerti da un servizio di Re-platform sono:

- ottimizzazione delle risorse e dei costi in quanto permette di utilizzare le caratteristiche dell'infrastruttura cloud senza richiedere modifiche significative agli applicativi;
- tempi di migrazione più rapidi rispetto a un refactoring completo;
- ottimizzazione delle caratteristiche del cloud in termini di disponibilità, scalabilità, osservabilità, resilienza, provisioning delle risorse e sicurezza rispetto ad un approccio lift&shift

#### 2.11.3.2 *Re-architect*

La strategia di Re-architect ha come obiettivo quello di adattare l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare i servizi cloud-native offerti dal PSN per massimizzare i benefici che ne derivano.



TIM - Uso Interno - Tutti i diritti riservati.

L'obiettivo è garantire i benefici attesi dall'Amministrazione e il minimo impatto per gli utenti finali. Il servizio si rende necessario, ad esempio, quando il livello di sicurezza è molto distante dallo standard minimo e realizza la modifica di moduli applicativi di un'applicazione al fine di garantirne un adeguato livello di sicurezza

Il servizio sarà disegnato rispettando i principi di design cloud-native che non solo consente di favorire la flessibilità operativa dei servizi applicativi, ma consente anche:

- un maggior riuso e velocità di implementazione
- l'utilizzo di metodologie consolidate di test (quanto più automatici) sia per le verifiche funzionali, sia per quelle di qualità e sicurezza
- l'uso di best practices di sviluppo e di progettazione (definite dal PSN) che consenta la trasformazione del codice applicativo in modo controllato
- una progettazione secondo le metodologie Secure by design

Discorso analogo vale per il monitoraggio delle applicazioni a valle di un progetto di "re-architect". L'adozione matura di metodologie cloud-native permette all'applicazione di usufruire di piattaforme comuni di monitoraggio e manutenzione proattiva.

Di seguito vengono illustrati i diversi step del processo di Re-architect.

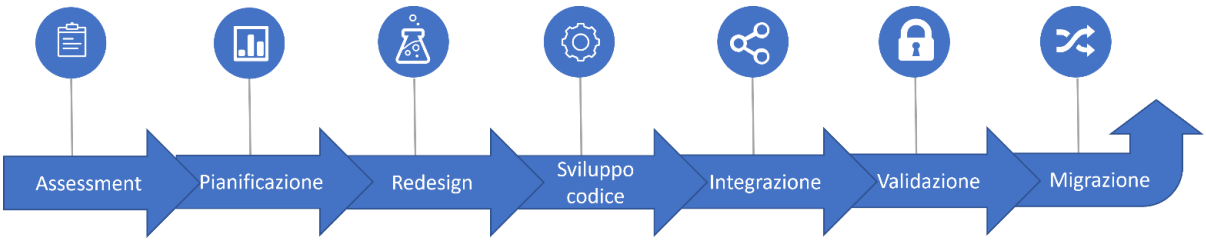



**Figura 15: Flusso processo di Re-architect**

Nella fase di *Assessment* viene analizzata l'applicazione per comprenderne le caratteristiche in modo da valutarne se la strategia di Re-architect sia adatta per quella specifica applicazione.
In particolare, alcune delle caratteristiche che vengono analizzate sono:

- frequenza di modifiche del codice;
- variabilità dei carichi di lavoro dovuto a picchi di traffico;
- criticità dal punto di vista business;
- architettura completa e Stack tecnologico utilizzato;
- uso di componenti sostituibili con l'equivalente servizio cloud-native;
- disponibilità e modificabilità del codice sorgente;
- criticità legate a componenti sostituibili con un'alternativa cloud native;



TIM - Uso Interno - Tutti i diritti riservati.

- disponibilità di documentazione tecnica completa del codice sorgente.

Dopo l'*Assessment* dell'applicativo, segue una fase di *Pianificazione* di migrazione, seguita da un *Redesign* minimale dell'applicazione per permettere una efficace migrazione. Le fasi successive comprendono interventi sul codice sorgente (*Sviluppo*) nei punti più critici che ostacolano il porting nel PSN, la verifica delle *Integrazioni* necessarie, la *Validazione* della nuova soluzione e, infine, la migrazione dell'applicazione sulla piattaforma PSN.

I vantaggi offerti da un servizio di Re-architect sono i seguenti:

- ottimizzazione dei costi e delle risorse nel lungo termine grazie all'utilizzo delle risorse basato sull'effettiva necessità;
- migliore sfruttamento delle caratteristiche del cloud come disponibilità, scalabilità, osservabilità, resilienza, provisioning delle risorse e sicurezza;
- responsività alle variazioni di carico impreviste grazie ad uno scaling in real time, possibile sulla nuova soluzione;
- incremento della sicurezza grazie anche alla disponibilità di funzionalità avanzate, fornite nella nuova piattaforma PSN.

### 2.11.4 Professional Services

La NewCo PSN renderà disponibili i servizi professionali sia nell'ottica del mantenimento ed accompagnamento della PA in un percorso evolutivo di IT Digital Transformation, sia in quello di proposizioni maggiormente innovative compresi i servizi legati al rifacimento/sviluppo applicativo.

La NewCo PSN prevede l'erogazione di servizi di Demand Management finalizzati alla raccolta e alla strutturazione delle esigenze di evoluzione e sviluppo dei processi, dei servizi e dei progetti delle Amministrazioni aderenti al PSN. Le attività di Demand Management prevedono l'identificazione e la comprensione dei requisiti di business delle strutture organizzative dell'Amministrazione, al fine di renderli coerenti rispetto alla strategia di evoluzione generale dell'Amministrazione. L'analisi dei requisiti abilita inoltre la definizione delle priorità, rispetto a criteri di scelta concordati con l'Amministrazione, in ottica di efficientamento e generazione di valore aggiunto.

In particolare, il servizio prevede l'esecuzione delle seguenti principali attività:

- Supporto nell'interazione di alto livello con le strutture organizzative per la definizione delle strategie, degli obiettivi e delle direttrici di evoluzioni dei processi, dei servizi e delle applicazioni;
- Conduzione di processi strutturati di raccolta e stesura, in forma strutturata e standardizzata, dei macro-requisiti progettuali;
- Identificazione e valutazione dei requisiti di business e delle esigenze espresse dalle strutture organizzative dell'Amministrazione;



TIM - Uso Interno - Tutti i diritti riservati.

- Valutazione, di concerto con l'Amministrazione, dell'aderenza di quanto realizzato rispetto ai requisiti raccolti e di coerenza rispetto a tempi e costi di implementazione delle soluzioni

In seguito all'avvenuta migrazione, la NewCo PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni. Pertanto, l'Amministrazione potrà decidere di affidare alla NewCo PSN la gestione dell'ambiente tenendo per sé solamente la componente relativa al codice applicativo. Per il corretto svolgimento delle attività verrà reso disponibile, per ogni PA, un Service Manager; un professionista di esperienza che coordina la gestione dei servizi di gestione contrattualizzata, operando a diretto contatto con l'Amministrazione. È responsabile della qualità del servizio offerto, e costituisce un punto di riferimento diretto del cliente per analisi congiunte del servizio, escalation, chiarimenti, personalizzazioni.

Le attività che la NewCo PSN potrà prendere in carico, previa valutazione, sono:

- ✓ Monitoraggio;
- ✓ Workload management;
- ✓ Infrastructure optimization;
- ✓ Capacity management;
- ✓ Operation management;
- ✓ Compliance management;
- ✓ Vulnerability & Remediation;
- ✓ Supporto tramite la Cloud Management Platform al:
  - Provisioning, Automazione e Orchestrazione di risorse;
  - Inventory, Configuration Management.

Inoltre, potranno essere erogate attività di System Management sui sistemi operativi Microsoft e Linux e sugli ambienti middleware effettuando la gestione ordinaria e straordinaria dei Server e dei Sistemi Operativi:

- ✓ creazione/gestione delle utenze, dei privilegi e gli accessi ai sistemi;
- ✓ controllare il corretto funzionamento del Sistema Operativo, verificando i processi/servizi tramite agent di monitoring.
- ✓ gestione dei log di sistema e verifica delle eventuali irregolarità.
- ✓ gestione dei files di configurazione dei sistemi.
- ✓ problem management di 2° livello, attivando le procedure e gli strumenti necessari per l'analisi dei problemi, individuando e rimuovendo le cause degli stessi.
- ✓ effettuare il restore in caso di failure di sistema recuperando i dati di backup.



TIM - Uso Interno - Tutti i diritti riservati.

- ✓ segnalazione dell'esigenza dell'applicazione di patch/fix per il mantenimento dei sistemi agli standard di sicurezza e qualità previsti dai produttori software (segnalazione periodica o eccezionale a fronte di gravi vulnerabilità).
- ✓ applicazione delle patch/fix, sulla base di quanto concordato con il cliente o a seguito di segnalazione dagli enti deputati alla sicurezza dei sistemi e dei Data Center.

Per tali servizi verrà proposto un **team mix** composto dal mix dei profili professionali sopra elencati, in base all'ambiente dell'Amministrazione ed ai requisiti della stessa.

### 2.11.5 Scenari di Migrazione

La strategia di migrazione si basa su un concetto di tailoring per definire il miglior processo di migrazione da proporre all'Amministrazione.

I driver per il tailoring sono:

**1. Dimensione dell'amministrazione.** Si ipotizza la seguente classificazione:
- ✓ PA di piccole dimensioni: fino a 10 Rack;
- ✓ PA di medie dimensioni: fino a 20 Rack;
- ✓ PA di grandi dimensioni: oltre 20 Rack.

**2. Livello di maturità dell'Amministrazione,** in base alle risultanze del Cloud Maturity Model.

| 0 - Legacy | 1 - Iniziale | 2 - Opportunistico | 3 - Sistematico | 4 - Misurabile | 5 - Ottimizzato |
|---|---|---|---|---|---|
| Le applicazioni (Legacy) vengono erogate da infrastrutture dedicata<br><br>Nessun servizio Cloud è stato ancora implementato | Alcuni settori o uffici hanno iniziato ad implementare servizi in cloud | È stato identificato un approccio di adozione, ma è applicato in modo opportunistico e non sistemistico<br><br>Sono stati ottenuti alcuni vantaggi iniziali | È stato consolidato un approccio di adozione del cloud che risulta sempre o quasi sempre adottato nel contesto operativo | È stata predisposta una infrastruttura di governance che gestisce e misura quantitativamente i servizi cloud | Tutti i servizi in cloud sono gestisti proattivamente<br><br>Sono stati implementati servizi su cloud federati o inter-cloud |

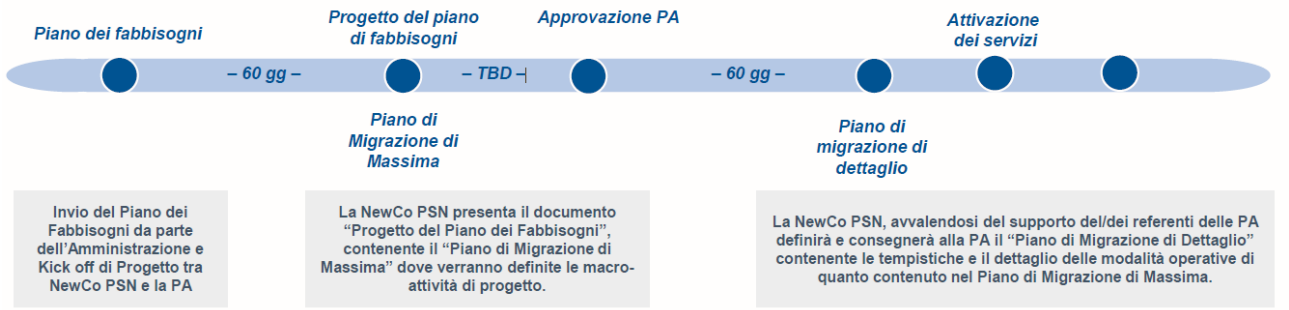
In base ai driver, il tailoring può dare luogo a 3 differenti scenari di complessità: bassa, media, alta.

Per quanto attiene alle tempistiche previste per il piano di migrazione, in figura una proposta a titolo esemplificativo che può essere declinata in funzione di diversi scenari:

| | | *Dimensione PA* | | |
|---|---|---|---|---|
| | | Piccola | Media | Grande |
| *Cloud Maturity* | 0 - Legacy | media | alta | alta |
| | 1 - Iniziale | media | media | alta |
| | 2 - Opportunistico | bassa | media | alta |
| | 3 - Sistemistico | bassa | media | media |
| | 4 - Misurabile | bassa | bassa | media |
| | 5 - Ottimizzato | bassa | bassa | bassa |



TIM - Uso Interno - Tutti i diritti riservati.




**Scenario 1 alta complessità.** Il "Piano di Migrazione di Dettaglio" dovrà evidenziare gli aspetti logistici, infrastrutturali, organizzativi e procedurali previsti per l'erogazione di quanto contenuto nel Piano di Migrazione di Massima, nonché la pianificazione temporale con cui verranno effettuate le attività.

**Scenario 2 media complessità**. Il Piano conterrà anche la proposta di migrazione/evoluzione a medio termine.

**Scenario 3 bassa complessità.** Il Piano conterrà anche le proposte di migrazione/evoluzione a medio e lungo termine.

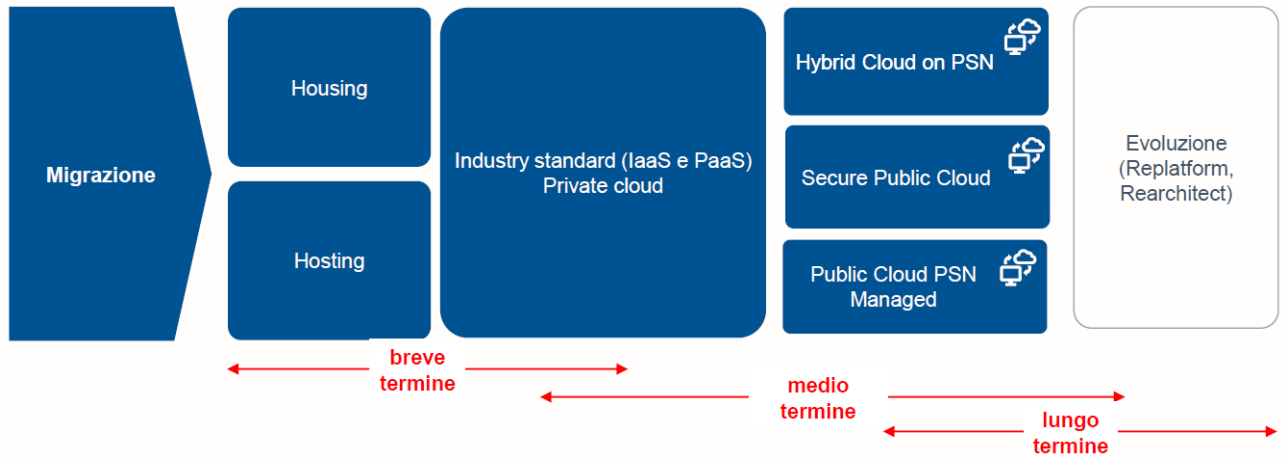
In base al livello di maturità dell'Amministrazione e alle necessità di classificazione dati, si proporrà un diverso Piano di Migrazione.

**Breve termine**
Ad eccezione dei casi di Housing, la migrazione sarà effettuata principalmente in modalità Re-Host (lift&Shift) che consiste nel "prendere" (Lift) l'intero servizio, compreso di infrastruttura, architettura, dati e traffico e "spostarlo" (Shift) su un hosting cloud senza modifiche al core dell'applicativo.

**Medio e lungo termine**
Questa strategia permette di effettuare un primo passo verso il cloud lasciando aperta la possibilità, successivamente, di implementare ulteriori miglioramenti all'applicativo che consentano di sfruttare ulteriormente i vantaggi del cloud andando ad utilizzare altre strategie di migrazione nel **medio e lungo termine** previste dal paradigma delle 6R, ossia Re-Platform e Re-Architect.



TIM - Uso Interno - Tutti i diritti riservati.




La NewCo PSN renderà disponibili alle Amministrazioni servizi di evoluzione con l'obiettivo di:

- ✓ **migliorare** eventuali ambienti precedentemente migrati sulla piattaforma PSN tramite Re-Host o tramite i servizi di Housing/Hosting;

| | | *Piano di Migrazione* | | |
|---|---|---|---|---|
| | | **Breve termine** | **Medio termine** | **Lungo Termine** |
| ***Cloud Maturity*** | **0 - Legacy** | Housing / Hosting | Hosting / Industry standard Private cloud | Evoluzione (Replatform, Rearchitect) |
| | **1 - Iniziale** | Hosting | Hosting / Industry standard Private cloud | Evoluzione (Replatform, Rearchitect) |
| | **2 - Opportunistico** | Hosting / Industry standard Private cloud | Industry Standard Private Cloud | Evoluzione (Replatform, Rearchitect) |
| | **3 - Sistemistico** | Hosting / Industry standard Private cloud | Industry Standard Private Cloud | Evoluzione (Replatform, Rearchitect) |
| | **4 - Misurabile** | Hosting / Industry standard Private cloud | Evoluzione (Replatform, Rearchitect) | Evoluzione (Replatform, Rearchitect) |
| | **5 - Ottimizzato** | Hosting / Industry standard Private cloud | Evoluzione (Replatform, Rearchitect) | Evoluzione (Replatform, Rearchitect) |
| | | **Hybrid Cloud on PSN** | | |
| | | **Secure Public Cloud** | | |
| | | **Public Cloud PSN Managed** | | |

- ✓ **supportare** la migrazione di applicativi on premise verso una piattaforma cloud tecnologicamente avanzata, in modo da beneficiare delle funzionalità messe a



TIM - Uso Interno - Tutti i diritti riservati.

disposizione dall'infrastruttura proposta, come sicurezza, scalabilità e ottimizzazione di costi e risorse.

### 2.11.6 Servizio opzionale di moving fisico

Il servizio di Housing descritto al § 2.1 del presente documento, prevede che la consegna degli apparati da ospitare presso il Data Center della Newco sia in carico al cliente.
Come elemento aggiuntivo opzionale, la NewCo PSN offre la possibilità alle PA che ne faranno richiesta, di fruire di un servizio di trasloco (Asset Moving), spostamento di asset in gestione, verso il sito PSN presso il quale sarà stato contrattualizzato l'Housing degli asset. Le macro-attività comprese nel servizio includono:

- verifica del back-up della macchina, lo smontaggio dell'apparato nella sede di partenza, lo spostamento inclusi i costi di assicurazione e di trasporto, il rimontaggio dell'apparato nella sede di destinazione, il cablaggio per la connessione alla rete, il collaudo della funzionalità dell'apparato, più ogni altra attività necessaria all'abilitazione della piena operatività del sistema;
- eventuali sopralluoghi nelle sedi di partenza e di destinazione necessari alla presa in carico dell'attività, all'identificazione delle eventuali criticità e alla definizione di accordi operativi con i Referenti dell'amministrazione contraente.

Il servizio è sottoposto ad alcuni vincoli, in particolare:

- il cliente deve garantire la possibilità di movimentazione in sicurezza degli apparati dalla sala server al piano stradale;
- il servizio non si fa carico di eventuali condizioni sulla manutenzione posta dai vendor in caso di movimentazione dell'asset.

## 2.12 Business & Culture Enablement

La trasformazione digitale deve essere accompagnata non solo da una innovazione tecnologica, ma soprattutto da un cambiamento delle metodologie di lavoro e dall'organizzazione dello stesso. Cambiare la cultura delle Amministrazioni vuol dire agire sulla leadership e sulla collaborazione tra le persone.

Disegnare e produrre servizi e prodotti per i cittadini e per l'imprese completamente digitali, vuol dire anche lavorare allo stesso modo; l'attenzione alle persone ed ai servizi loro erogati consente infatti di rendere questa cultura normale all'interno dell'Amministrazione e quindi poterla replicare più facilmente per i cittadini e le imprese.

Punti nodali di questa trasformazione sono il change management ed il modello formativo. Per questi motivi, la NewCo PSN prevede di mettere a disposizione delle amministrazioni entrambi questi servizi.

Per quanto riguarda il Change Management si prevede un servizio di consulenza organizzativa che progetterà con le Amministrazioni i passi per eseguire il processo di digital trasformation relativamente a:

- Modello organizzativo.



TIM - Uso Interno - Tutti i diritti riservati.

- Competenze e modello manageriale.
- Tool Collaborativi.
- Employee experience.
- Modello di innovazione.

Inoltre. un servizio che consente di erogare formazione tramite l'uso delle tecnologie multimediali e offrire la possibilità di erogare digitalmente i contenuti attraverso Internet o reti Intranet. Per l'utente rappresenta una soluzione di apprendimento flessibile, in quanto personalizzabile e facilmente accessibile.

Il servizio prevede l'erogazione, su una piattaforma messa a disposizione dal PSN, di **corsi base** a catalogo differenziati in base alle esigenze formative e **corsi personalizzati** secondo le esigenze dell'Amministrazione. In aggiunta ai due servizi precedentemente indicati se ne definisce uno di **supporto specialistico** per gli ulteriori aspetti metodologici e didattici, che prevede:

- affiancamento all'utente volto ad istruirlo all'uso delle funzioni del sistema di e-learning;
- gestione della comunicazione con gli utenti tramite i sistemi di messaggistica della piattaforma;
- formazione trasversale con corsi specifici definiti a catalogo e/o customizzati su esigenze dell'Amministrazione su:
    - servizi Cloud ed elementi di innovazione ed ottimizzazione
    - migrazione e analisi degli adeguamenti normativi e degli standard come quelli descritti, ad esempio, nei programmi di Digital Transformation indicati da AgID;
    - formazione verticale su metodologie e processi Cloud, necessarie per governare gli ambienti ed i servizi;
    - formazione su tecnologie Cloud illustrando i vantaggi/benefici di tale servizio;
    - formazione specifica a supporto degli ambienti implementati e dell'offerta degli strumenti del PSN

Inoltre, il PSN renderà disponibile la piattaforma ed il supporto specialistico per i seguenti ambiti:

- amministrativo/organizzativo
- tecnologico

L'area amministrativo/organizzativo prevede i seguenti servizi base:

- validazione e controllo dei risultati delle elaborazioni;
- aggiornamento e manutenzione del data base;
- reportistica e monitoraggio.

L'area tecnologica prevede i seguenti servizi base:



TIM - Uso Interno - Tutti i diritti riservati.

- processi di creazione, classificazione e archiviazione dei contenuti della piattaforma;
- gestione del repository dei contenuti della piattaforma: gestione del ciclo di vita e delle versioni dei contenuti, gestione degli accessi, supporto per contenuti multimediali;
- caricamento di nuovi corsi di auto addestramento e/o aggiornamento di corsi esistenti;
- attività di gestione delle utenze interne/esterne al sistema di e-learning.

Per i corsi ad hoc è previsto un servizio di predisposizione del materiale didattico (realizzazione di WBT) che adotterà standard di mercato per la produzione (learning object, SCORM, ecc...) e logiche di interattività e di costo differenziate, così come indicato nel documento AgID per la realizzazione dei contenuti didattici. Tra questi si distinguono:

- corsi base di tipo generale: usualmente si trovano nei cataloghi dei vari fornitori e fanno riferimento a temi di utilità comune; si prevede di erogare corsi a catalogo con pacchetti da 8 WBT ognuno.
- corsi ad hoc a bassa, media e alta interazione in accordo con le metriche indicate da AgID.

In base alle necessità delle singole amministrazioni verrà individuato il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste.



TIM - Uso Interno - Tutti i diritti riservati.

# 3 Sicurezza

La NewCo PSN si doterà di idonee unità organizzative al fine di garantire e assicurare la tutela delle infrastrutture e dei servizi considerati essenziali agli interessi nazionali e alla sicurezza nazionale; in particolare, istituirà al suo interno una Organizzazione di Sicurezza, con elementi caratteristici di autonomia e indipendenza. Tale unità sarà anche preposta alle attività aziendali rilevanti per la sicurezza nazionale e ne sarà garantito il coinvolgimento nelle attività di governance, in particolare riguardo ai processi decisionali afferenti ad attività strategiche e di interesse nazionale.

Il responsabile di tale organizzazione potrà essere individuato in accordo con le autorità istituzionali competenti e dotato di specifici requisiti (es. NOS, cittadinanza italiana).

L'Organizzazione di Sicurezza garantirà la conformità e avrà l'obiettivo di:

- garantire una protezione dell'informazione adeguata in termini di confidenzialità, integrità e disponibilità;
- proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- assicurare la conformità alle leggi e ai regolamenti applicabili, tra cui quelle inerenti la sicurezza delle informazioni, la tutela dei dati personali nonché quelle applicabili agli Operatori dei Servizi Essenziali (OSE), ai Fornitori di Servizi Digitali (FSD) ed ai soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC);
- assicurare un modello strutturale alla protezione dell'informazione e alla gestione dei rischi correlati;
- rispondere in modo efficace alle crescenti minacce ai sistemi informativi nello spazio cibernetico.

Le misure tecniche ed organizzative dovranno essere identificate ed implementate ai sensi delle normative vigenti; saranno inoltre soggette a certificazione ISO/IEC 27001 e ISO 22301 e saranno descritte da specifiche Security Policy elaborate a cura dell'Organizzazione di Sicurezza, in particolare con riferimento alla sicurezza e alla conformità dei sistemi informatici e delle infrastrutture delle reti.

Nel dettaglio, tali Security Policy, che rappresentano gli obiettivi ed i principi di base che devono essere rispettati nella conduzione dei servizi oggetto della fornitura, saranno definite in conformità alle normative applicabili e elencate al § 3.1. Le regole, le procedure operative ed organizzative attuative delle suddette Policy saranno invece riportate nelle procedure di cui al § 3.3.

Il Centro Servizi si impegna inoltre a offrire un continuo miglioramento dei processi attuati in aderenza alle Security Policy di cui sopra e un utilizzo ottimale delle risorse impiegate.

L'Organizzazione di Sicurezza predisporrà uno specifico e dettagliato Piano di Sicurezza redatto in conformità con i criteri di accreditamento AgID relativi ai PSN, che conterrà i) una sintesi delle normative di riferimento applicabili; ii) una generale ricognizione degli asset informatici; iii) le criticità anche potenziali, gli obiettivi di sviluppo, manutenzione e gestione atti a garantire la



TIM - Uso Interno - Tutti i diritti riservati.

corretta erogazione dei servizi; *iv)* le risorse strumentali ed economiche necessarie. In aggiunta saranno integrati elementi relativi alle modalità logistiche ed organizzative, agli strumenti ed ai sistemi che la NewCo PSN adotterà o di cui è provvisto per rendere sicuro e protetto l'ambiente in cui sono ospitati le infrastrutture (Data Center).

Tale Piano sarà revisionato e aggiornato con cadenza almeno annuale e, comunque, ogniqualvolta si dovessero presentare evenienze tali da generare modifiche delle esigenze di sicurezza nella erogazione dei servizi oggetto di fornitura ascrivibili a *i)* ragioni organizzative, procedurali, tecnologiche; *ii)* ad eventuali input della revisione ciclica del sistema di gestione; *iii)* a indicazioni provenienti dai processi di gestione della sicurezza e dall'analisi dei rischi di sicurezza. Tale attività di aggiornamento si svilupperà anche al fine di indirizzare il miglioramento continuo del livello di efficienza dei processi di sicurezza e alla Mission del Centro Servizi.

All'Organizzazione di Sicurezza saranno inoltre attribuiti compiti di controllo e supervisione in relazione alla corretta implementazione nei vari ambiti operativi del Centro Servizi, secondo quanto indicato dalle Security Policy; esse saranno opportunamente definite secondo procedure periodicamente aggiornate. Il personale deputato ad effettuare tali attività di verifica potrebbe essere abilitato secondo criteri definiti dagli organi istituzionali competenti (es. dotati di NOS) e avrà il compito di effettuare, secondo modalità e termini definiti, le verifiche per l'accertamento della sussistenza dei requisiti di sicurezza.

In particolare, saranno eseguite attività di analisi del rischio di sicurezza:

a. nell'ambito dei progetti, per la identificazione dei requisiti di protezione e controllo;

b. sui servizi di erogazione per verificare l'adeguatezza dei controlli in essere, identificare eventuali scostamenti ed identificare le azioni di rientro.

L'analisi dei rischi dovrà essere ripetibile e condotta mediante appositi strumenti di valutazione che permettano anche il tracciamento delle azioni di rimedio eventualmente identificate.

Per ciascuno dei tre modelli di cloud saranno garantiti livelli equivalenti di sicurezza; per il Secure Public Cloud saranno utilizzati i controlli di sicurezza disponibili dal Public Cloud Provider, con l'aggiunta, se necessario, di quelli ulteriori individuati dall'analisi del rischio e dalle necessità di conformità normativa.

Sul piano delle operations, l'Organizzazione di Sicurezza, svilupperà, in particolare, le funzioni di Security Operation Center (SOC) e di Computer Emergency Response Team (CERT) e garantirà tutti i livelli di sicurezza previsti dalle normative vigenti (cfr. par 3.1), la presenza di un ambiente sicuro e protetto e la protezione dei dati personali trattati.
In generale saranno svolte le seguenti attività a contenuto operativo:

- End Point Security;
- Identity & Access Management;
- Key Management;



TIM - Uso Interno - Tutti i diritti riservati.

- Security Platform Management;
- Security Policy Management & Enforcement;
- Real Time Security Monitoring;
- Security Testing & Vulnerability Management;
- Threat Intelligence&Infosharing;
- Incident Response;
- Training & Awareness;

In generale l'Organizzazione di Sicurezza, si farà carico di tutte le attività di progettazione e set up della Gestione della Sicurezza IT, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

## 3.1 Normative e standard di riferimento

Tenendo in considerazione le esigenze di sicurezza di una infrastruttura dedicata a fornire servizi Cloud e l'evoluzione costante del contesto tecnologico/normativo fortemente enfatizzata dalla recente pubblicazione di direttive, regolamenti, norme e decreti a livello UE e nazionale, il Centro Servizi messo a disposizione dalla NewCo PSN dovrà implementare i più avanzati standard di sicurezza delle informazioni e garantire la conformità, propria e dei propri clienti, ai requisiti cogenti.

Le principali esigenze di sicurezza riguardano:

- la presenza di un ambiente sicuro e protetto;
- la protezione dei dati personali trattati;
- la conformità normativa e di settore del Centro Servizi e dei clienti;

L'erogazione dei servizi ed i sistemi coinvolti soddisferanno pienamente, quindi, i seguenti dispositivi di legge:

- **D.Lgs. 7 marzo 2005, n. 82 e s.m.i** ("Codice dell'Amministrazione Digitale");
- **Piano Triennale per l'Informatica 2020 – 2022** ("Piano triennale per l'informatica nella Pubblica Amministrazione");
- **DPCM del 17/02/2017** («Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali»);
- **D. Lgs. 65/2018 e s.m.i.**, che attua la direttiva UE 2016/1148 (Direttiva «NIS»), intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, applicati agli «Operatori di Servizi Essenziali» (OSE) e ai «Fornitori di Servizi Digitali «(FSD);
- **D.L. 105/2019** (convertito con modificazioni dalla L. 18 novembre 2019, n. 133), come adeguato a sua volta dalla legge n. 8 del 28 febbraio 2020 e dal D.L. 82/2021, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, e i DPCM (tra



TIM - Uso Interno - Tutti i diritti riservati.

cui il 131/2020, entrato in vigore il 5/11/2020) e regolamenti di successiva emanazione (alla data DPR 54/2021 e DPCM 81/2021), come previsti dalla menzionata legge;

- **DPCM n. 131 del 30 luglio 2020** "Regolamento in materia di Perimetro di Sicurezza Nazionale Cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";
- **DPCM n. 81 del 14 aprile 2021** "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;
- **DPR n. 54 del 5 febbraio 2021** "Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
- **DPCM 15 giugno 2021** "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;"
- **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*Regolamento Generale sulla Protezione dei Dati o GDPR*);
- **D.Lgs. 196/2003**, modificato dal D.Lgs. 10 agosto 2018, n. 101 ("Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE");
- **D.L. 65/2018, "**Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
- **D.L. 82/2021 (convertito con modificazioni dalla L. 4 agosto 2021, n. 109)** "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale";

Saranno inoltre considerati come standard di realizzazione e gestione le seguenti linee guida e framework nazionali/internazionali:

- **Piano nazionale per la protezione cibernetica e la sicurezza informatica;**
- **Framework nazionale di cyber security e data protection;**
- **NIST Cyber Security Framework;**
- CIRCOLARE N. 2 del 9 aprile 2018 **Criteri per la qualificazione dei Cloud Service Provider per la PA;**



TIM - Uso Interno - Tutti i diritti riservati.

- CIRCOLARE N. 01 del 14 giugno 2019 **Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;**
- **Misure minime** di sicurezza informatica per la PA (AgID GG.UU 4/2017);
- **ISO/IEC 27000** (Adozione, Implementazione e gestione di un Sistema di Gestione per la Sicurezza delle Informazioni, ed in particolare:
    - **ISO/IEC 27001** – Information technology — Security techniques — Information security management systems — Requirements;
    - **ISO/IEC 27002** - Information technology — Security techniques — Code of practice for information security controls;
    - **ISO/IEC 27701** – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines;
    - **ISO/IEC 27017** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
    - **ISO/IEC 27018 -** Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
    - **ISO/IEC 27005** - Information technology — Security techniques — Information security risk management;
- **ISO 31000:2018** - Gestione del rischio - Linee guida;
- **Cloud Security Alliance** Controls;

Tutti i membri della NewCo PSN sono in possesso della certificazione, in corso di validità, del Sistema di Gestione per la Sicurezza delle informazioni relativamente a tutti i Centri Servizi presso i quali sarà prestato il Servizio – rilasciata in conformità alla ISO/IEC 27001 da un ente di certificazione accreditato da ACCREDIA o da altro ente di Accreditamento firmatario degli accordi di Mutuo riconoscimento.

## 3.2 Personale e Competenze

Il personale che sarà utilizzato dalla NewCo PSN per la governance e la gestione della sicurezza avrà elevate conoscenze e competenze in materia di Cyber Security, in base al profilo utilizzato, nonché esperienza lavorativa nel settore.

Le risorse impiegate nell'ambito del progetto saranno di alto profilo, sotto l'aspetto dell'esperienza, delle conoscenze e delle competenze. In particolare, saranno impiegati profili di tipo Master, Senior o Expert, laddove richiesto, con competenze multidisciplinari di sicurezza.

Le risorse avranno ampia esperienza e conoscenza adeguata nei seguenti campi:



TIM - Uso Interno - Tutti i diritti riservati.

- Sicurezza delle informazioni: networking, infrastrutture di rete, indirizzamento, architetture di elaborazione, gestione dei database, infrastrutture di sicurezza, endpoint management, strutture client-server, ecc.
- Monitoraggio e controllo: effettuazione delle operazioni di controllo, tramite strumenti automatici o mediante analisi manuale del corretto funzionamento degli apparati; controllo della corretta configurazione delle infrastrutture; identificazione e classificazione degli eventi in relazione alle tipologie di allarmi scatenati.
- Gestione degli incidenti: gestione delle emergenze, governo rapido ed efficace delle operazioni di contenimento degli incidenti di sicurezza in ambito IT, cooperazione con le altre linee di business.

I profili saranno corredati dalle necessarie certificazioni, in funzione dei ruoli svolti. Come regola generale, le risorse dovranno possedere alcune tra le seguenti tipologie di certificazioni, in base al ruolo ricoperto:

- Capo Progetto: PMP o Prince2;
- Specialisti di Governance: CISM, CRISC, ISO/IEC 27001 Lead Auditor;
- Technical Head e Security Architect: CISSP, CISA, CISM, ITIL, e certificazioni tecniche di prodotto;
- Specialisti di prodotto: altre certificazioni specialistiche di prodotto;

Le procedure di formazione e aggiornamento delle aziende del NewCo PSN assicurano l'allineamento delle conoscenze e delle competenze dei profili al mercato e la garanzia di formazione continua per far fronte al rischio di obsolescenza anche delle competenze stesse.

## 3.3 Processi di gestione della sicurezza

L'obiettivo della NewCo PSN è contrastare le minacce che possano mettere a repentaglio le informazioni delle Amministrazioni e l'erogazione dei servizi oggetto della fornitura. Per il raggiungimento di tale obiettivo, la NewCo si impegna a gestire la sicurezza delle informazioni garantendone la Riservatezza, l'Integrità e la Disponibilità attraverso il rispetto e l'attuazione delle Security Policy che saranno descritte nel Piano della Sicurezza.
In particolare, le regole, le procedure operative ed organizzative attuative delle suddette Security Policy saranno riportate in specifiche procedure di gestione della sicurezza IT conformi allo standard ISO/IEC 27002, in linea con quanto prescritto dall'Allegato A della Circolare AgID nr 1 del 14 giugno 2019 in tema di PSN nonché delle normative elencate nel § 3.1, tra cui si ricordano quelle inerenti la tutela dei dati personali e quelle applicabili agli Operatori di Servizi Essenziali (OSE) ed ai soggetti inclusi.

Tra queste procedure rientrano a titolo esemplificativo le seguenti:

- procedura per la classificazione delle informazioni;
- procedura per la gestione degli asset, ivi incluso quanto prescritto dal DPCM nr 131/2020 in materia di Perimetro di Sicurezza Nazionale Cibernetica, che richiede la comunicazione



TIM - Uso Interno - Tutti i diritti riservati.

all'autorità competente dell'Elenco dei Beni ICT inclusi nel perimetro e dell'Analisi del Rischio;

- procedura per il controllo degli accessi logici;
- procedura per la gestione della sicurezza fisica ed ambientale;
- procedura per la gestione dei cambiamenti;
- procedura per la gestione del back-up;
- procedura per la gestione dei log;
- procedura per la gestione delle vulnerabilità tecniche;
- procedura per la gestione della sicurezza della rete;
- procedura per la gestione della sicurezza nei processi di acquisizione, sviluppo e manutenzione dei sistemi. Con riferimento al processo di acquisizione si terrà conto anche di quanto prescritto dal DPR nr 54/2021 in materia di Perimetro di Sicurezza Nazionale Cibernetica e suoi regolamenti attuativi, che definiscono le procedure, modalità e termini di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di valutazione (CV);
- procedura per la sicurezza delle terze parti;
- procedura per la gestione degli incidenti di sicurezza, ivi incluso quanto prescritto dal DPCM n. 81/2021 in materia di Perimetro di Sicurezza Nazionale Cibernetica, che definisce le modalità di notifica degli incidenti aventi impatto sui Beni ICT perimetro al CSIRT Italia. In particolare, il decreto individua i tipi di incidenti cibernetici per i quali è obbligatoria la notifica al CSIRT Italia, dividendoli in due categorie sulla base della gravità dell'incidente stesso e stabilendo diverse tempistiche per la relativa notifica. Gli incidenti cibernetici che rientrano nei 19 tipi considerati meno gravi (categoria A) devono essere notificati al CSIRT entro 6 ore, mentre quelli che rientrano nei 6 tipi considerati più gravi (categoria B) entro un'ora, con l'obbligo di integrare tempestivamente quanto comunicato in caso di conoscenza di elementi aggiuntivi (salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa). Al contempo, è possibile notificare, su base volontaria, anche i tipi di incidenti non elencati nel decreto.

## 3.4 Tecnologie e Best Practices

Le tecnologie impiegate per garantire la protezione dei dati e per estensione delle infrastrutture a supporto dei servizi erogati saranno scelte con le garanzie di:

- allineamento con il mercato per l'adozione di tecnologie di sicurezza di tipo COTS o Open Source largamente diffuse e accreditate come leader di mercato allo scopo di massimizzare l'efficacia, la facilità d'uso e al contempo ridurre i rischi di lockdown tecnologico;
- riuso di esperienze già fatte con altri clienti nella stessa area di mercato o in aree affini;



TIM - Uso Interno - Tutti i diritti riservati.

- sistemi open che garantiscono la massima compatibilità con eventuali altre tecnologie IT e/o di sicurezza che potranno essere introdotte in seguito.

In fase di progettazione saranno garantite, secondo le principali best practice, la protezione delle infrastrutture IT e di rete, nonché la protezione delle informazioni in esse memorizzate, implementando le architetture e i controlli di seguito descritti.

L'implementazione delle best practice e dei controlli di sicurezza sarà parte integrante della realizzazione della sicurezza by design dei due centri Private Cloud. Per quanto riguarda il Secure Public Cloud ne sarà puntualmente verificato con il Cloud Provider l'utilizzo, ed eventualmente realizzati dei piani di conformità addizionali, se necessari.

Il PSN fornirà la **gestione della sicurezza** in accordo alle responsabilità tradizionalmente definite all'interno di tutti i modelli IaaS e PaaS previsti nel presente progetto, come riportato nella figura seguente:

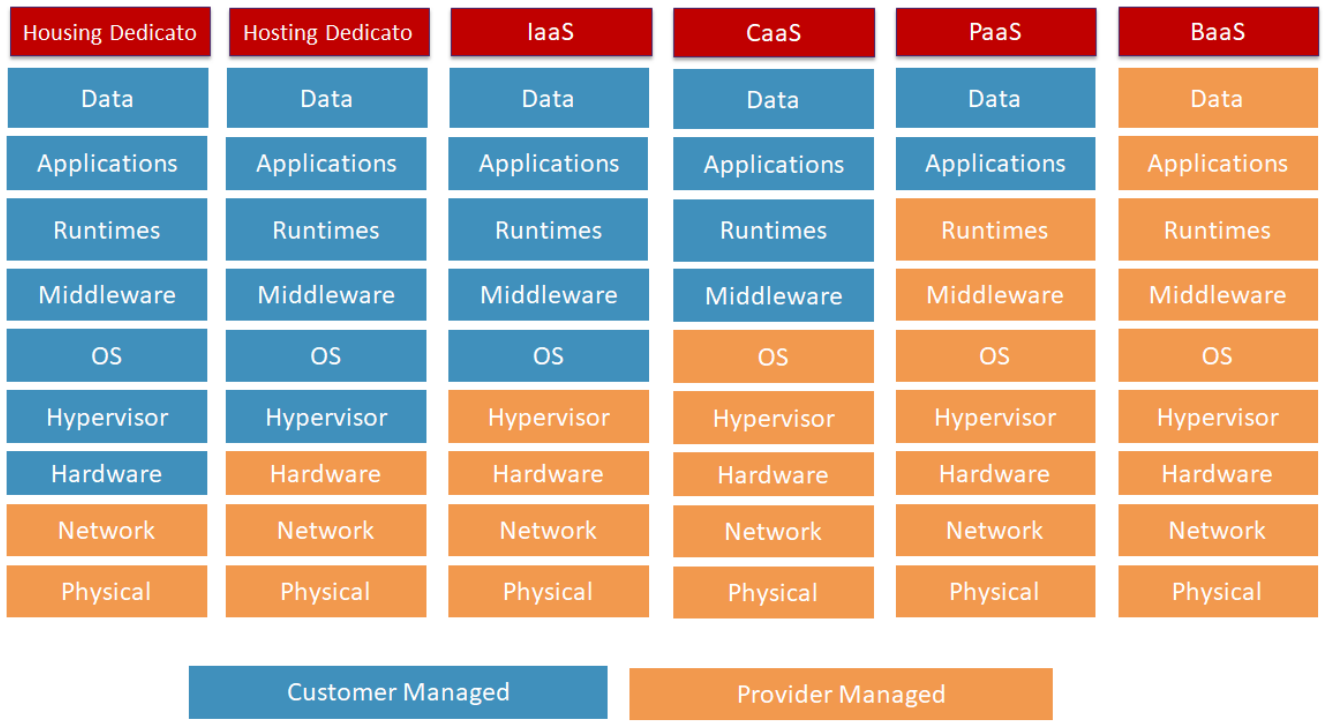



**Figura 16: Gestione della Sicurezza**

Nei paragrafi seguenti le componenti fondamentali di sicurezza che saranno implementate all'interno del PSN.

## 3.5 Infrastructure Security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.



TIM - Uso Interno - Tutti i diritti riservati.

La sicurezza delle infrastrutture è in carico al PSN, nei limiti di quanto espresso in Figura 15 – Gestione della Sicurezza.

Il Centro Servizi sarà realizzato prevedendo le seguenti soluzioni ed infrastrutture di sicurezza IT:

- **Segregazione degli ambienti**: soluzioni e procedure per garantire la segregazione degli ambienti elaborativi a seconda della categorizzazione e della rischiosità delle attività ivi condotte e del livello di criticità dei dati trattati, garantendo l'applicazione del principio di difesa in profondità. Sarà garantita la separazione fisica, di rete e logica in accordo ai criteri di classificazione identificati (rischiosità attività, dati trattati e difesa in profondità) e assicurata la relativa coerenza. Per i servizi di Housing e Hosting sarà realizzata la segregazione dei sistemi e delle reti a livello di tenant di tipo logico tramite VLAN e subnetting. Per i servizi XaaS sarà realizzata la segregazione dei sistemi e delle reti tramite tecnologie di Software Defined Network (SDN).
- **Accesso ai sistemi di elaborazione:** soluzioni I&AM per garantire che l'accesso verso gli ambienti elaborativi, con criteri di accesso restrittivi verso quelli più critici e rilevanti per la natura dei dati trattati, ad esempio accessibili attraverso macchine dedicate, collocate su una rete logicamente dedicata. Tali macchine non potranno essere utilizzate per altre attività e presenta configurazioni di sicurezza del tipo: accesso con autenticazione a due fattori, restrizioni delle attività rischiose (es. ricezione/invio di email), logging abilitato. Per i servizi di Housing, l'accesso ai sistemi di elaborazione è a carico dell'Amministrazione.
    - **Security logging:** soluzioni e procedure per assicurare la registrazione e la tracciabilità delle operazioni sui sistemi e le componenti di rete. Le soluzioni e le procedure adottate garantiranno che gli accessi degli utenti ai sistemi informativi siano sempre registrati in un apposito file di log di cui è necessario assicurare le caratteristiche di completezza, inalterabilità e possibilità di verifica della integrità delle registrazioni. I log saranno raccolti tramite uno strumento di log management ai fini di "audit", "prevention" e "detection" di minacce alla sicurezza dei dati, con inclusione di quelli personali. Tutti i dispositivi ed in particolare quelli che producono dati di tracciamento avranno l'orologio interno sincronizzato con i sistemi centralizzati (ad esempio connettendosi a GPS o NTP affidabili). Le relative connessioni saranno protette da interferenze e manomissioni. Per i servizi di Housing e Hosting il logging dei sistemi è a carico dell'Amministrazione, mentre quello degli apparati di rete è a carico del PSN.
- **Security Hardening:** Il Data Center prevede procedure di configurazione sicura dei sistemi in modo da minimizzare la superficie di attacco attraverso la rimozione dei servizi non strettamente necessari e per quelli rimanenti, assicurare che le parametrizzazioni di sicurezza siano correttamente implementate. Gli standard di Hardening saranno basati su fonti riconosciute, tra le quali, a titolo esemplificativo: www.nist.gov, www.sans.org e www.cisecurity.org, www.iso.org e i fornitori di prodotti. Per i servizi di Housing e di Hosting, l'Hardening dei sistemi di elaborazione è a carico dell'Amministrazione.
- **Sicurezza dei sistemi elaborativi:** Il Data Center sarà dotato di strumenti, procedure e personale qualificato per assicurare la protezione dei sistemi elaborativi tramite software di end point protection e end point detection & response. Per i servizi di Housing e Hosting



TIM - Uso Interno - Tutti i diritti riservati.

l'Hardening dei sistemi di elaborazione è a carico dell'Amministrazione. Per i servizi XaaS è a carico dell'amministrazione la protezione dei Sistemi Operativi in caso di IaaS, mentre è a carico del PSN nel caso di PaaS, CaaS e SaaS, nei limiti di quanto stabilito in Figura 15 Gestione della Sicurezza.

## 3.6 Network security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture, reti e archivi adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.

La sicurezza dell'infrastruttura di rete è a carico del PSN e include la sicurezza di tutti i servizi on top ai servizi Cloud, quali Help Desk e Contact Center, NOC, SOC e CERT, CMP, Portali di accesso e gestione, infrastruttura interna di amministrazione e gestione dell'infrastruttura del Cloud Center.

Il Centro servizi sarà protetto con tecnologie di protezione delle reti che includono quelle specificate di seguito.

- **Network Security:** strumenti, procedure e personale per gestire le richieste di definizione di regole di filtraggio del traffico IP (Network Firewall), con relativi workflow di approvazione e in maniera auditabile. Regolare review delle regole firewall deve essere garantita con periodicità di almeno 6 mesi.
- **NGFW e/o IDS/IPS:** strumenti NGFW e/o IDS/IPS allo stato dell'arte per controllare il traffico ingoing e outgoing dall'ambiente ospitato con relativi workflow di approvazione e in maniera auditabile. Regolare review delle regole di sicurezza deve essere garantita con periodicità di almeno 6 mesi.
- **Network Access Control (NAC):** strumenti di controllo e autenticazione degli endpoint che si connettono alla rete. Supporterà lo standard 802.1X e ulteriori meccanismi di autenticazioni (es. certificati digitali). Assicurerà controlli preventivi sulla sicurezza dell'host per la compliance dei dispositivi alle policy di sicurezza.
- **Accesso Zero Trust:** soluzioni e procedure che consentano l'accesso remoto tecnologie che implementano l'accesso mediante paradigma Zero Trust.
- **Web Application Firewall (WAF):** strumenti WAF allo stato dell'arte per controllare il traffico ingoing e outgoing dagli ambienti elaborativi. L'infrastruttura WAF sarà ridondata ed in alta affidabilità. Le policy di detection dei WAF saranno definite in relazione alle funzionalità applicative e le vulnerabilità applicative di riferimento (es. OWASP) e saranno regolarmente aggiornate in relazione alle evoluzioni dell'applicazione che protegge.
- **E-mail & Web Security**: strumenti di protezione e-mail e Web (Secure E-mail Gateway e Secure Web Gateway) per la protezione del traffico e-mail e web relativamente al personale del centro, con relativi workflow di approvazione e in maniera auditabile. Sarà assicurata la disponibilità di strumenti di contrasto avanzato di APT e minacce zero-day tramite l'utilizzo di funzionalità di sandboxing.
- Tutti i dispositivi saranno configurati per inviare i log delle attività alla piattaforma di log management. I log saranno raccolti tramite uno strumento di log management ai fini di



TIM - Uso Interno - Tutti i diritti riservati.

"audit", "prevention" e "detection" di minacce alla sicurezza dei dati, con inclusione di quelli personali.

## 3.7 Data Security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture, reti e archivi adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.

Il Centro servizi sarà protetto con tecnologie di protezione avanzata dei dati che includono:

- **Data discovery and classification:** Il Centro Servizi per assicurare una maggiore protezione dei dati disporrà di soluzioni, procedure e personale assicurano un presidio di data discovery e di data classification, contribuendo alla Data Governance. Attraverso gli strumenti e le procedure di data discovery si mirerà a scoprire dati strutturati e non in modo che siano classificati e protetti.
- **Data at rest encryption:** Il Centro Servizi adotterà strumenti e procedure per garantire la protezione dei dati quando salvati sui dischi in uso per lo storage dei dati. La cifratura dei dischi sarà implementata in accordo con le principali best practice e standard (es. NIST Special Publication 800-57 Part 1, FIPS, PCI DSS).
- **Data in transit protection:** Il Centro Servizi impiegherà strumenti e procedure per assicurare la protezione della riservatezza dei dati quando in transito, con particolare attenzione alla comunicazione via reti pubbliche. La cifratura delle comunicazioni includerà diversi meccanismi riconosciuti come standard di settore, come ad esempio IPSEC, TLS.
- **Database encryption:** Il Centro Servizi per assicurare una maggiore protezione dei dati a livello di archiviazione fisica, ossia dati archiviati e file di registro, impiegherà strumenti e procedure per assicurare la cifratura dei database. La soluzione potrà assicurare la crittografia in tempo reale dei database senza dover modificare le applicazioni che li usano.
- **Data masking:** Il Centro Servizi al fine di assicurare che i dati più critici siano solo disponibili in ambiente di produzione e che siano rispettati i vincoli di minimizzazione dei dati utilizzerà soluzioni e procedure atte a creare copie sicure e protette dei dati mediante l'anonimizzazione e la crittografia delle informazioni che potrebbero minacciare la privacy, la sicurezza o la conformità dei dati.

Le aree di controlli tecnologici che saranno implementate all'interno del Centro Servizi saranno a copertura delle aree descritte nei seguenti paragrafi (SOC/CERT), in cui viene dettagliato il relativo servizio.

## 3.8 SOC

Per realizzare i servizi erogati dal SOC, la NewCo PSN metterà a disposizione un Security Operation Center dal quale saranno erogati i servizi di gestione operativa della sicurezza. La Control Room del SOC sarà localizzata esternamente ai centri servizi del PSN. L'infrastruttura da gestire, che implementa i controlli tecnologici che proteggono le infrastrutture a supporto dei servizi saranno



TIM - Uso Interno - Tutti i diritti riservati.

invece ospitate all'interno dei Data Center. I servizi SOC saranno disponibili in orario continuato (8x5) più reperibilità.

Il servizio di Security Monitoring sarà disponibile in finestra oraria estesa (24x7).

Dal SOC saranno erogati i servizi di gestione delle piattaforme di sicurezza utilizzate all'interno dei Centri Servizi, descritti nei seguenti paragrafi.

### 3.8.1 End Point Protection

La NewCo PSN disporrà di strumenti, procedure e personale qualificato per assicurare la gestione della sicurezza degli End Point utilizzati per lo svolgimento delle attività lavorative e, ove applicabile per i servizi di hosting e X-aaS, per tutte le funzionalità necessarie per l'erogazione degli stessi.

Le tecnologie a supporto del servizio di gestione della sicurezza degli End Point avranno le seguenti funzionalità:

- Crittografia dei dischi;
- Software di protezione antivirus (AV), costantemente aggiornato, e con inibita, salvo impossibilità tecniche, la possibilità di disabilitare l'antivirus da parte degli utenti;
- Software di Data Loss Prevention, per identificare, monitorare e proteggere i dati in uscita dagli endpoint attraverso l'intercettazione e il blocco;
- Software di protezione avanzata denominato Endpoint Detection & Response che operi in modo integrato con le difese antivirus (AV) e metta a diposizione funzionalità di (a) analisi del comportamento e machine learning per bloccare attività malevole, (b) gestione degli indicatori di compromissione (IOC), e (c) produzione delle evidenze per l'analisi forense;
- Personal firewall e device control;
- Gestione dei dispositivi mobili attraverso soluzione di Mobile Device Management (MDM).
- File Integrity Monitoring

Sono esclusi servizi di End Point Security degli endpoint interni ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. Macchine Virtuali).

### 3.8.2 Identity and Access Management

La NewCo PSN disporrà di strumenti, procedure e personale qualificato per il governo degli accessi logici, la gestione e il controllo degli accessi privilegiati ai sistemi, meccanismi di autenticazione semplice e multifattoriale e servizi di federazione delle identità.

Il SOC dovrà erogare servizi di sicurezza inerenti alla gestione degli accessi logici che includano:

- **Identity and Access Governance:** Il Data Center avrà strumenti, procedure e personale qualificato per assicurare la gestione e il controllo del ciclo di vita delle identità logiche. Dovranno essere presenti procedure e meccanismi di provisioning e deprovisioning delle



TIM - Uso Interno - Tutti i diritti riservati.

utenze sui diversi target e, ove possibile, meccanismi di automazione delle relative attività. Dovrà essere assicurata l'univocità degli account e le relative password devono essere individuali. Dovranno essere presenti procedure e meccanismi di richiesta di accesso logico con relativi workflow di approvazione. Sarà assicurata la cessazione delle identità logiche non appena non vi siano più le condizioni che ne rendono necessaria la definizione (es. cessazione del rapporto di lavoro). Dovranno essere presenti procedure e meccanismi atti ad effettuare la revisione periodica degli accessi per assicurare che le abilitazioni rilevate siano in linea con il ruolo di business.

- **Privileged Access Management:** Il controllo delle utenze privilegiate attraverso la memorizzazione delle relative credenziali in vault logici e la registrazione delle sessioni amministrative verso i target. Saranno presenti procedure e meccanismi di provisioning e deprovisioning delle utenze privilegiate con relativi workflow di approvazione. Le attività di gestione delle utenze privilegiate dovranno essere registrate e le registrazioni collezionate centralmente presso un sistema di analisi e correlazione eventi (SIEM). La infrastruttura della soluzione di gestione e controllo delle utenze privilegiata dovrà garantire ridondanza e alta affidabilità.
- **Authentication Management:** Il Data Center avrà strumenti, procedure e personale qualificato per assicurare la gestione delle credenziali di accesso in linea con gli standard e le best practice di settore.
- **Identity Federation services:** Il Data Center avrà strumenti per assicurare la federazione delle identità attraverso meccanismi standard e industry best practice (es. SAML e OAUTH).
- **Multi-factor Authentication:** Il Data Center sarà dotato di strumenti, procedure e personale qualificato per assicurare che l'accesso logico possa avvenire con meccanismi aggiuntivi alla password in linea con la definizione di 2 factor authentication definita dagli standard e dalle best practice di settore.

L'erogazione del presente servizio è prevista per il funzionamento del presente progetto in favore dei clienti che usufruiscono dei servizi di Hosting e XaaS. Sono esclusi servizi di I&AM per le utenze interne ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. account e/o user su Macchine Virtuali).

### 3.8.3 Key Management

La NewCo PSN assicurerà la gestione delle chiavi crittografiche e dei certificati digitali relativamente ai servizi erogati in modalità Hosting e XaaS.

Tale servizio sarà conforme a quanto indicato nelle pubblicazioni NIST 800-57.

Il SOC garantirà soluzioni, procedure e personale qualificato per la gestione delle chiavi crittografiche simmetriche e asimmetriche in accordo con le principali best practice e standard (es. NIST Special Publication 800-57 Part 1, FIPS, PCI DSS).

Il servizio avrà le seguenti caratteristiche:



TIM - Uso Interno - Tutti i diritti riservati.

- Le procedure di gestione delle chiavi dovranno assicurare il dual control e lo split knowledge, oltre che la piena tracciabilità nell'uso e nella gestione delle chiavi, in linea con gli standard e le best practice di settore (es. NIST, PCI DSS).
- Le chiavi di cifrature conservate dentro key store cifrati (e.g., a FIPS 140-2 Level 3 compliant hardware security module).
- I ruoli e le responsabilità dei custodi delle chiavi crittografiche saranno documentati e conosciuti
- Il personale incaricato opererà in piena segregazione organizzativa, fisica, operativa
- Le procedure dovranno regolamentare l'intero ciclo di vita delle chiavi, ossia la gestione della generazione, scambio, archiviazione, utilizzo, crypto-shredding (distruzione) e sostituzione delle chiavi
- I certificati digitali saranno gestiti attraverso specifica piattaforma che comprende il monitoraggio delle scadenze.

L'erogazione del servizio è prevista per il funzionamento del presente progetto e in favore dei clienti che usufruiscono dei servizi di Hosting e XaaS. É esclusa la gestione delle chiavi interne ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. certificati SSH su Macchine Virtuali).

### 3.8.4 Security Platform Management

Il SOC garantirà il servizio di Security Platform Management che si applica alle seguenti piattaforme:

- End Point Security;
- I&AM;
- Key Management;
- Network Firewall;
- Next Generation Firewall e IDS/IPS;
- Web Application Firewall;
- Secure E-mail Gateway;
- Secure Web Gateway;
- Data Loss Prevention;
- SIEM/SOAR;
- Network & Zero Trust Access Control.

Il servizio assicura:

- La gestione di tutte le piattaforme di sicurezza;
- La manutenzione evolutiva e correttiva delle piattaforme di sicurezza, compresi upgrade e applicazione delle patch e hotfixes;



TIM - Uso Interno - Tutti i diritti riservati.

- La verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma.

### 3.8.5 Security Policy Management & Enforcement

Il SOC garantirà il servizio di security Policy Management & enforcement, assicurando:

- La gestione di tutte le richieste di implementazione/modifica policy di sicurezza sulle piattaforme di sicurezza inclusive di:
  - Network Firewall;
  - Next Generation Firewall e IDS/IPS;
  - Web Application Firewall;
  - Secure E-mail Gateway;
  - Secure Web Gateway;
  - Data Loss Prevention;
  - SIEM/SOAR;
  - Network & Zero Trust Access Control.
- Il controllo dell'efficacia delle contromisure di sicurezza attive sul dispositivo.

### 3.8.6 Log Management

Il SOC garantirà il servizio di Log Management tramite un'infrastruttura di log collection & archiving.

I log saranno raccolti in modalità agent based or agentless e archiviati all'interno di una piattaforma di log management e protetti da modifica, cancellazione e distruzione, nonché accessibili solo da personale autorizzato. I sistemi saranno configurati per evitare la sovrascrittura degli eventi. I log e gli eventi di sicurezza saranno resi disponibili e trasferiti alla infrastruttura preposta alla loro analisi e correlazione. La ritenzione dei file di Log rispetterà le normative applicabili.

Il SOC si occuperà della gestione della piattaforma e di:

- assicurarsi della corretta raccolta dei log dalle sorgenti in perimetro;
- effettuare la verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma;
- verificare la corretta archiviazione dei log;
- rendere disponibili i log su richiesta;
- supportare procedure e sessioni di audit, nonché attività di gestione di incidenti di sicurezza;



TIM - Uso Interno - Tutti i diritti riservati.

- effettuare la verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma.

### 3.8.7 Security Monitoring

La NewCo PSN erogherà servizi che mirano al monitoraggio del livello di sicurezza delle informazioni per la pronta rilevazione di incidenti o anomalie di sicurezza.

Saranno utilizzati strumenti, procedure e personale qualificato per assicurare il monitoraggio in tempo reale del livello di sicurezza delle infrastrutture, rilevare ed eventualmente investigare le anomalie di sicurezza e gestire in caso di necessità la risposta alle gravi minacce e agli incidenti.
Il team sarà composto da analisti e specialisti di sicurezza suddivisi in 1° e 2° livello e organizzati per assicurare il presidio continuativo e l'attivazione del personale specialistico in reperibilità negli orari extra lavorativi.

Il presidio di primo livello sarà organizzato in combinazione con altre funzioni di gestione operativa se adeguate in termini di strumenti e personale qualificato.

Al fine di garantire efficacia per il rilevamento e monitoraggio degli incidenti di sicurezza, il SOC utilizzerà strumenti di **Security Information and Event Management (SIEM).** Tale strumento consente l'analisi e la correlazione degli eventi di sicurezza per garantire la individuazione di eventi sospetti o anomali. Tale piattaforma concentrerà le registrazioni di sicurezza originate dalle soluzioni di sicurezza e dall'intera infrastruttura. Specifiche dashboard ed allarmi saranno rese disponibili per assicurare il monitoraggio della sicurezza della intera infrastruttura, includendo applicazioni, sistemi e reti. Lo strumento raccoglierà i log dalla piattaforma di log management o direttamente dai sistemi di elaborazione e dalle piattaforme di sicurezza.

## 3.9 CERT

Per realizzare i servizi erogati dal CERT la NewCo PSN metterà a disposizione un CERT esterno dal quale saranno erogati i servizi di sicurezza reattivi e proattivi. Anche la control room del CERT sarà localizzata esternamente ai centri servizi del PSN. L'infrastruttura da gestire, che implementa i controlli tecnologici che proteggono le infrastrutture a supporto dei servizi saranno invece ospitate all'interno dei Data Center. I servizi CERT saranno disponibili in orario lavorativo 09.00-18.00 dal lunedì al venerdì, garantendo reperibilità nel restante periodo.

La NewCo PSN assicurerà la risposta agli attacchi di tipo cibernetico attraverso strumenti, procedure e personale focalizzati alla valutazione degli scenari di minaccia, la rilevazione degli attacchi e il coordinamento delle azioni di risposta agli incidenti di sicurezza tramite una struttura dedicata e organizzativamente separata da quelle di gestione (IT, SOC).

Per assicurare un'appropriata segregazione dei ruoli, questo team non potrà includere il personale operativo che ha in gestione l'infrastruttura da monitorare, assicurando la necessaria terzietà del controllo.
Al fine di garantire efficacia nella pronta individuazione delle minacce e nella risposta agli incidenti di tipo cibernetico, il CERT del Data Center dovrà avere le seguenti caratteristiche minime:



TIM - Uso Interno - Tutti i diritti riservati.

- avere relazioni formali e riconosciute con CERT rilevanti (es. Polizia Postale/CNAIPIC, CSIRT Italia e CERT AgID);
- dotarsi di procedure di cyber security incident che in linea con gli standard e le best practice di settore includano gli step necessari alla classificazione, contenimento, analisi delle cause, e radicamento e notifica verso le Autorità, oltre che raccolta delle eventuali evidenze forensi;
- promuovere campagne di awareness e prevedere simulazioni in ambito sicurezza cibernetica allo scopo di valutare la readiness nella risposta a minacce e incidenti siffatti.

In questo ambito rientrano i servizi descritti nei successivi paragrafi.

### 3.9.1 Threat Hunting

Il CERT per rilevare segnali deboli che possono indicare la compromissione delle infrastrutture, degli ambienti elaborativi o la compromissione di un utente tramite una capacità di Threat Hunting, che permette di indentificare comportamenti anomali o associati a tecniche tattiche e procedure note di attacco.

### 3.9.2 Threat intelligence & Infosharing

La NewCo PSN sfrutterà servizi avanzati di Threat intelligence & Information Sharing e adotterà strumenti, procedure e personale per assicurare competenze predittive in ambito sicurezza cibernetica.

Nel farlo verranno attivati servizi di intelligence che consentano di:

- scambiare informazioni in forma anonimizzata su nuove tecniche di attacco (TTPs) e scenari di minaccia;
- scambiare informazioni in forma anonimizzata, anche in forma di IOC (Indicator of Compromise) su incidenti di sicurezza cibernetica occorsi;
- ricevere notifiche e allarmi su minacce di Cyber (es. zero-day, campagne di malware, pandemie digitali, attori e incidenti)

Per verificare in maniera capillare e tempestiva la presenza di indicatori di compromissione, sarà necessario dotare il Centro Servizi di strumenti di IoC automation basati sull'integrazione di:

- piattaforme open-source (es. MISP Open Source Threat Intelligence and Sharing Platform – precedentemente nota come Malware Information Sharing Platform);
- software di protezione avanzata denominato Endpoint Detection & Response come descritto nel paragrafo 3.8.1End Point Protection;
- strumenti di log management in grado di correlare ed allarmare la presenza di SOC sia in real-time che sullo storico dei log con congrua profondità.



TIM - Uso Interno - Tutti i diritti riservati.

### 3.9.3 Security Testing & Vulnerability Management

I Data Center avranno strumenti, procedure e personale per gestire le attività di testing delle infrastrutture, valutarne i relativi risultati, identificare e indirizzare le strategie di mitigazione.

Il Data Center utilizzerà strumenti, procedure e personale per gestire le attività di testing delle infrastrutture e valutarne i relativi risultati. Dato che un'adeguata protezione dalle minacce di sicurezza necessita di un approccio sistematico e continuativo, sarà prevista l'esecuzione periodica di sua serie di verifiche e test di sicurezza (Vulnerability Assessment e Penetration Test), al fine di mantenere i livelli di rischio residuo in linea con i requisiti (es. OWASP).

Il Data Center garantirà una adeguata copertura delle attività di testing, prevedendo come requisiti minimi:

- Vulnerability assessment almeno trimestrali dall'esterno e dalle reti interne in corrispondenza dei front end;
- Penetration test infrastrutturale dall'esterno con cadenza semestrale;

Al fine di rimediare le eventuali vulnerabilità riscontrate il Data Center adotterà le procedure di gestione delle vulnerabilità in linea con le best practices di settore e i principali standard di sicurezza (es. CIS, SANS, PCI DSS).

Queste prevedono che la classificazione delle vulnerabilità avvenga secondo standard internazionali (es. CVSS) e le attività di rimedio siano proporzionate al livello di esposizione al rischio introdotto dalle vulnerabilità.

### 3.9.4 Incident Response

L'Incident Response è un servizio erogato dal CERT in risposta agli incidenti di sicurezza. La risposta sarà attivata dai processi di monitoraggio SOC, dalla verifica di segnalazioni di Threat Intelligence o da richiesta interna o di terze parti. Il servizio prevede un'investigazione di dettaglio che permette di definire la migliore strategie di risposta e coordinare i vari gruppi necessari per indirizzare la parte di rimedio.

Le attività principali sono atte a isolare i sistemi compromessi, preservare e non alterare le evidenze digitali, verificare l'occorrenza e la causa ultima dell'evento analizzato e indicare le corrette metodologie per eradicare la minaccia e ripristinare i sistemi effetti. A completare il servizio si effettua attività di malware analysis e/o analisi forense ove richiesta.

Per realizzare il servizio di security monitoring, sarà introdotta anche una piattaforma **SOAR** in uso dal CERT, per l'automazione delle procedure di security incident management e l'integrazione delle tecnologie utilizzate per la detection e la reazione.



TIM - Uso Interno - Tutti i diritti riservati.

# 4 Infrastruttura IT e Network

I Servizi elencati nel *§. 1.4 Oggetto della Fornitura* saranno erogati dal Centro Servizi della NewCo PSN in modalità "run", a meno del servizio di Migrazione che sarà attivato "una tantum". La finestra temporale di erogazione dei servizi in modalità "run" è 24H (00:00 – 24:00) per 365 giorni l'anno.

Dal momento della stipula del contratto, i Servizi verranno attivati e resi disponibili alle PA che li richiedano secondo quanto indicato nel presente documento, fermo restando che tutti i servizi, o parte di essi, ovvero anche uno solo di essi, potranno subire variazioni in aumento o in diminuzione.

In caso di guasto, la NewCo PSN è tenuta a ripristinare la perfetta funzionalità e la piena disponibilità dei Servizi oggetto di Fornitura, garantendone i tempi di ripristino secondo quanto previsto dagli indicatori di qualità definiti nell'allegato 1 del documento di "Specificazione delle caratteristiche del Servizio e della Gestione".

I Servizi di Infrastruttura IT consistono nella messa a disposizione, da parte della NewCo PSN, di tutti gli apparati hardware e software infrastrutturale necessari a garantire gli elevati standard qualitativi in termini di affidabilità e disponibilità nel rispetto dei requisiti indicati di seguito al ***paragrafo 4.1 Apparati Hardware e software infrastrutturale***.

La NewCo PSN si farà carico di tutte le attività di progettazione e set up dell'Infrastruttura IT, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

Di seguito sono riportate le infrastrutture IT impiegate per le diverse modalità di erogazione (Housing, Hosting e IaaS):

- **Server fisici**: l'infrastruttura della PA sarà ospitata esclusivamente su server **dedicati** tra PA che ne richiedano l'erogazione in tale modalità. L'erogazione del presente servizio è prevista nella sola modalità Hosting.
- **Server virtuali**: l'infrastruttura della PA virtualizzata sarà ospitata esclusivamente su server **condivisi** tra PA che ne richiedano l'erogazione in tale modalità. L'erogazione del presente servizio è prevista nella sola modalità IaaS
- **Storage**: l'insieme di dispositivi Hardware e Software messi a disposizione per l'immagazzinamento permanente dei dati. L'erogazione del presente servizio è prevista nelle modalità Hosting e IaaS.

## 4.1 Apparati Hardware e software infrastrutturale

### 4.1.1 High Level Design dell'architettura

Il modello di riferimento prevede una piattaforma Cloud che grazie a un global control plane consentirà di erogare servizi da diverse Regioni (Region) e relative zone di disponibilità (Availability Zones - AZ) in territorio italiano. Ciò consentirà quindi ad ogni PA di abilitare servizi aggiuntivi per la protezione di sistemi e dati, in modo da realizzare configurazioni in Business Continuity e/o in Disaster Recovery.



TIM - Uso Interno - Tutti i diritti riservati.

La singola PA potrà attingere a servizi Cloud disponibili in una qualunque Region e relativa AZ e potrà interconnetterli tra di loro grazie ad un Network Layer logico, unico e trasversale, realizzato sul paradigma del Software Defined Network.

Inoltre, la Cloud Platform avrà un «connettore» diretto verso i Cloud Service Provider *Hyperscaler* (Google, Microsoft, Oracle): tale connettore garantirà una funzione di Cloud Services Gateway per l'interfacciamento diretto e privato verso i servizi Cloud degli *Hyperscaler* (Service Brokering) da parte dei workload della PA ospitati nel Cloud PSN.

L'infrastruttura Cloud sarà ospitata all'interno di **4 Data Center distribuiti sul territorio italiano,** allestiti in una configurazione di **doppia *Region* (2 DC + 2 DC)**, e quindi ciascuna ridondata con una coppia di zone di disponibilità in alta affidabilità. I data center sono dotati di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire i massimi standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti.

La configurazione infrastrutturale è quindi completamente ridondata grazie alla suddivisione di ognuna delle due Region (Nord e Sud, distanti tra loro centinaia di chilometri) in *dual-AZ* (Availability Zone), cioè una coppia di Data Center in configurazione di business continuity, distanti tra loro diverse decine di chilometri in linea d'aria. In particolare, le due AZ sono interconnesse grazie ad un backbone proprietario che garantisce a sua volta completa ridondanza, latenza trascurabile e connettività privata, tale da caratterizzare la coppia logicamente come un unico Data Center virtuale (*Software Defined Data Center*).

Anche le Region sono interconnesse attraverso lo stesso backbone proprietario e da un Network layer in grado di consentire un'architettura di rete logica flessibile, Software Defined, che garantisca la mobilità dei carichi applicativi e l'alta affidabilità intrinseca delle soluzioni Cloud.

All'interno di una zona di disponibilità dunque i workload vengono distribuiti in maniera trasparente e la configurazione di HA (High Availability) consente di realizzare la continuità di servizio infrastrutturale (Business Continuity) tra i due data center della stessa Region (vedi documento specifico "*Specificazione delle caratteristiche del servizio e della gestione PSN_v11*" per le caratteristiche del servizio DR/BC offerto). Di fatto, grazie a questa configurazione di base, la piattaforma Cloud prevederà la distribuzione anche dei dati nelle due zone di ogni singola Region. Questa configurazione è possibile grazie alla distribuzione dello storage space (individuato in tecnologie di Storage Array tra le migliori disponibili sul mercato IT) all'interno delle due AZ e quindi grazie alla continuous data replication del servizio prescelto da ogni singola PA. In tal modo, qualora una singola PA decidesse di avvalersi della ridondanza completa della sua infrastruttura (fisica o virtuale che sia) potrà far leva sulla configurazione in HA della piattaforma Cloud e costruire così delle soluzioni di DR/BC.

La specificità della piattaforma Cloud, grazie al backbone proprietario di interconnessione delle due AZ costituenti ogni singola Region, permetterà la replica sincrona/asincrona dei dati tra i sistemi Storage Array costituenti lo Storage Layer.

In tale contesto operativo, la singola PA potrà beneficiare quindi della capacità intrinseca della piattaforma Cloud di reagire ad eventi disastrosi rendendo possibile la riattivazione dei workload all'interno di una delle due AZ o su una Region diversa. La ripartenza dei workload protetti dalla soluzione di DR/BC attivata, consentirà poi alla singola PA, in modo del tutto autonomo, la gestione del riavvio di ogni singola applicazione, secondo i propri piani di DR o di BC.



TIM - Uso Interno - Tutti i diritti riservati.

In caso di necessità, inoltre, la piattaforma Cloud prevede anche la disponibilità di backup di singoli componenti del workload della PA e dei relativi dati e, per protezione ulteriore, gli stessi backup possono essere trasferiti da una Region all'altra in modo tale che vi sia sempre una copia del dato disponibile in una delle due Region, al fine di poter avviare una restore in caso di necessità. Questa possibilità può essere utilizzata inoltre anche per esigenze di "*offsite vaulting*", ovvero per proteggere gli archivi di backup da eventi di disastro, replicandoli su una Region diversa (es. archivi di dati di cui occorra garantire la disponibilità a lunga conservazione per disposizioni normative): mentre le soluzioni di DR/BC si focalizzano sulla ripartenze dei servizi a fronte di eventi di disastro, e quindi sui dati correnti delle relative applicazioni, l'offsite vaulting si occupa quindi della protezione degli archivi di dati a lunga retention.

Le soluzioni tecnologiche in ambito Network WAN infine, garantiscono gli accessi remoti ai siti da parte di ogni singola PA e l'interconnessione fra i siti stessi. La piattaforma Cloud è quindi da intendersi come geograficamente distribuita e in grado di reagire a diverse situazioni di disservizio che dovessero generarsi durante il normale esercizio operativo.

Grazie a queste predisposizioni e configurazioni si potrà garantire, in base alle caratteristiche del servizio Cloud prescelto da una PA, la conformità a valori di RTO (Recovery Time Objective) e di RPO (Recovery Point Objective) per l'infrastruttura configurabili a seconda dell'esigenza, fino ai valori più stringenti disponibili e riportati nella seguente tabella:

| RTO | RPO |
|---|---|
| **30 minuti** | **1 minuto** |

In caso di soluzioni di continuità su Region distinte, ad esempio per implementazione di scenari di Disaster Recovery in grado di proteggere da eventi disastrosi come catastrofi naturali, la piattaforma Cloud sarà in grado di garantire valori di RTO e RPO almeno pari a:

| Scenario | RTO | RPO |
|---|---|---|
| **DR sito infrastrutturale** | **4 ore** | **30 minuti** |

La soluzione di DR resa disponibile prevede la possibilità di abilitare la configurazione di matrici di replica full-mesh tra tutti i DC costituenti le differenti Region. Ciò garantisce ad ogni PA la possibilità di scegliere di volta in volta la collocazione dei servizi più adatta alle proprie esigenze di workload (es. per prossimità geografica all'utenza, ecc) e delle relative istanze di replica.

### 4.1.2 Componente server

Il modello di architettura PSN si pone come obiettivo quello di essere standard dal punto di vista del Design architetturale a prescindere dal modello di servizio/offerta da erogare.
Basandosi su sistemi IT di tipo Blade Server configurabili tramite applicazione di Profili Logici predisposti per ogni esigenza in base al modello di erogazione del servizio/offerta, i singoli Blade server di tipo StateLess vengono profilati all'occorrenza sia dal punto di vista della configurazione HW che dell'OS/Hypervisor da installare per l'utilizzo finale.



TIM - Uso Interno - Tutti i diritti riservati.

Tutto questo è possibile grazie all'elevata standardizzazione e integrazione con il Network Layer e gli automatismi del Delivery automatico del Cloud Management Platform (CMP) che quindi consentono l'attivazione di server sia HW che virtuali.
Quindi, una volta effettuato l'iniziale Design Architetturale, integrati i sistemi Blade Server col Network Layer e con il CMP, non vi sarà alcun'altra progettazione da eseguire se non attivare, logicamente, nuovi profili di servizio per gli stateless system disponibili.

Il modello di architettura della NewCo PSN si propone come soluzione "**open**": architettura senza alcun tipo di **vendor Lock-In** e aperta alla potenziale creazione di tutte le possibili piattaforme progettate per l'erogazione di servizi ICT (*evitando di fatto l'acquisto di hardware ad hoc per ogni piattaforma di erogazione di un determinato servizio per il cliente finale*).

Il modello architetturale dell'Erogatore minimizza l'effort in termini di costi e tempi inerenti la Site Preparation perché la sua realizzazione è richiesta solo all'inizio («**one shot**»), durante la prima installazione del modello architetturale con i server di tipo Blade System e riutilizzata senza variazione alcuna per l'attivazione di nuovi Server Blade.

Dato l'utilizzo di Blade Server System ad alta standardizzazione, sarà possibile anche prevedere un preliminare predisposizione di spazi attrezzati nel DC al fine di ospitare nuovi Blade Server System di fatto riducendo il tempo necessario alle attivazioni di nuovi POD di erogazione di fatto migliorando il Time To Market per l'offerta di servizi ai clienti finali.

Eventuali esigenze di scalabilità dei Blade Server System, già installati in un DC, in termini di aggiunta banda di Uplink verso LAN e SAN, si riducono alla sola predisposizione di nuovi cablaggi in fibra ottica partendo da predisposizioni e configurazioni già create in precedenza e quindi di fatto semplificando anche questo eventuale insieme di attività.

La infrastruttura di computing sarà quindi basata su Blade System modulari che possano scalare orizzontalmente con la sola aggiunta di componenti Chassis e Blade Server in quanto la connettività LAN/SAN sarà predefinita e predisposta all'atto dell'attivazione e installazione del PoD (Point of Delivery).

La configurazione minima del Blade System avrà connettività LAN con multi interface da 10-100Gbps e SAN con multi interface 16-32Gbps.

Il sistema Blade Server System garantisce no SPOF e in particolare:

- alimentazione/alimentatori ridondati e di tipo hot-plug
- sistema di raffreddamento ridondato e di tipo hot-plug
- ridondanza di ogni modulo HW costituente lo Chassis ospitante i Blade Server così come tutto il Blade Server System
- Chassis/Blade Server Power Management (IPMI Enabled)
- HW/Chassis Management Module dell'intero Blade System ridondato e con connessione LAN Out of Band (ridondante) che consenta la completa configurazione/monitoraggio del sistema da remoto



TIM - Uso Interno - Tutti i diritti riservati.

Ogni Blade Server installabile e configurabile nel Blade System disporrà di:

- Minimo 2 socket CPU (CPU Intel o AMD con opzioni di risparmio energetico)
- Configurazione con almeno 16 core e multithreads enabled (parametri minimi: 2.5GHz/20-core/150W)
- Minimo 256GB di RAM e fino a 1TB di RAM

### 4.1.3 Componente storage

L'infrastruttura Storage prevista nell'architettura proposta è basata su Storage Area Network (SAN) fully redundant che consente connettività diretta Fiber Channel (FC) verso gli Storage Array Enterprise dai quali configurare storage space utile alla configurazione dei Blade Server (con relativo OS/Hypervisor).

La infrastruttura storage è in grado di erogare **80 PetaByte** e di scalare orizzontalmente in base alle esigenze dei clienti e delle relative infrastrutture durante tutto il loro ciclo di vita.
Il dato capacitivo si riferisce alla somma tra il dato live e la sua replica e la soluzione dovrà prevedere almeno il 20% di disco altamente prestazionale.

L'architettura storage infatti è in grado di garantire configurazione di tipo High Availability (HA) tra DC della stessa Region e abilitante al servizio di Disaster Recovery (DR) tra differenti Region con diversi SLA RTO/RPO disponibili (DRaaS).

L'architettura storage inoltre potrà erogare le seguenti modalità di servizio:

- Encryption;
- Configurazione "recovery automatico" sui due siti (HA);
- Thin Provisioning;
- Snapshot manager;
- Replica a tre siti (HA+DR);
- Automated Tiered anche su sito secondario;
- Connettività 32Gbps;
- Possibilità di passare da modalità sincrono ad asincrono (e viceversa) in maniera non distruttiva;
- Gestione, monitoraggio, reportistica, chargeback e storicizzazione delle performance.

### 4.1.4 Piattaforme software infrastrutturale

L'architettura di Blade System per il computing layer sarà disponibile per poter configurare sia Bare Metal Server con relativo OS (Microsoft Windows Server e/o Linux in different revision) sia Hypervisor (VMware e/o Red Hat Enterprise Virtualization e/o Oracle VM).



TIM - Uso Interno - Tutti i diritti riservati.

In tal modo sarà possibile andar a definire per ogni cliente il disegno architetturale voluto e necessario per garantire migrazione del workload preesistente presso i DC e ottimizzazione delle configurazioni grazie alla possibilità di consolidamento tecnologico su Blade System di nuova generazione e con capacità computazionali allineate agli ultimi rilasci tecnologici.

### 4.1.5 Backup standard

La NewCo PSN renderà disponibile un'infrastruttura Hardware e Software e un insieme di Standard e Linee Guida, comuni a tutti i DC di Servizio, per l'effettuazione delle attività di Backup e Restore.

Il servizio sarà reso disponibile attraverso un'unica console centralizzata dalla quale è possibile gestire la protezione dei propri dati attraverso un backup efficace e sicuro con un Restore rapido. Tale console consente la gestione in piena autonomia (in modalità self managed) della protezione dei dati permettendo quindi l'esecuzione di jobs di backup e restore dei svariati contesti (filesystem, virtual machine, database and application, posta elettronica, ecc) del cliente in modo efficace e sicuro.

I contesti da proteggere a cui è applicabile tale soluzione possono essere di varia tipologia (Files, VM, Container (k8), tutti i principali database come SAP-HANA, Exchange, SQL, Oracle, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, o i principali PaaS).

Il servizio garantisce al Cliente totale autonomia per il salvataggio dei propri dati e naturalmente il recupero degli stessi, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software. Il ripristino può avvenire ad una certa data in relazione alle copie di backup effettuate. Il servizio di backup standard prevede di effettuare il backup dello storage base (100GB) previsto per ogni istanza.

Il servizio si basa su dei backup server che coordinano ed eseguono tutte le operazioni di backup e remote vaulting. Sulla base delle schedulazioni pianificate, il backup server esegue i jobs di backup. In particolare, il Backup server avvia, sulla base delle schedulazioni programmate, la connessione tra gli agent presenti sui sistemi (Sistemi operativi o hypervisor/cloud) e i Mediagent presenti presso il Data Center Primario e i Data Center secondari per consentire il backup delle VM e/o dei dati (Database, filesystem AIX, ecc.).

Per tutti i backup sarà effettuata una ulteriore copia secondaria al completamento della copia primaria presso il Data Center secondario.

Trattandosi di un servizio «self-managed» l'utente ha completa autonomia di gestione nella definizione della policy di backup. All'attivazione del servizio al referente tecnico (comunicato in fase di acquisizione del servizio) saranno inviate le credenziali di accesso alla console del servizio. Alla mail del referente tecnico saranno inviate tutte le mail inerenti alle informazioni del servizio.

Le principali caratteristiche del servizio che verrà realizzato sono:

- La possibilità di effettuare backup full e incrementali;
- Cifratura dei dati nella catena end to end (dal client alla libreria);



TIM - Uso Interno - Tutti i diritti riservati.

- Possibilità di organizzare i backup ed effettuare ricerche sulla base di differenti filtri (es. date di riferimento) e mantenere più backup in contemporanea;
- Possibilità di poter selezionare cartelle e file da sottoporre a backup e possibilità di escludere tipologie di file per nome, estensione e dimensione per i backup di tipo file system (con installazione di un agent sui server oggetto di backup);
- la conservazione e svecchiamento dei dati del back-up secondo policy di retention standard: 7 giorni, 1 mese, 2 mesi, 3 mesi, 6 mesi, 1 anno, 10 anni;
- possibilità di modificare la policy di retention (tra quelle su indicate) applicate ai backup;
- monitoring dei jobs di backup e restore;
- reportistica all'interno della console;
- un metodo efficiente per trasmissione ed archiviazione applicando tecniche di compattazione e compressione ed identificando ed eliminando i blocchi duplicati di dati durante i backup.
- Il ripristino dei dati scegliendo la versione dei dati da ripristinare in funzione della retention applicata agli stessi.
- il ripristino granulare dei dati (singolo file, mail, tabella, ecc.) in modalità "a caldo e out-of-place" garantendo quindi la continuità operativa. Tale modalità di ripristino assicura la possibilità di effettuare dei test di restore in qualsiasi momento e con qualsiasi cadenza.
- Repository storage del servizio su apparati di tipo NAS o S3 (AWS-S3 compatibile)
- GDPR Compliant: Supporta utente e ruoli IAM oltre alla cifratura del dato e controllo degli accessi

## 4.2 Network

Costituisce oggetto della presente fornitura la messa a disposizione delle Interconnessioni e della connettività network del presente Progetto di fattibilità.

I Data Center oggetto di Fornitura prevedono componenti di Data Center Interconnection (DCI) tramite interfacce DWDM, di Virtual Local Area Network prevedendo una portata di Traffico, ruotata nei Data Center cifrata su suolo pubblico.

Il degrado delle caratteristiche trasmissive rispetto ai valori richiesti e sopra riportati o l'interruzione fisica della fibra ottica verranno considerate entrambe come guasto.

La NewCo PSN si farà carico di tutte le attività di progettazione e set up della Connettività, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.
Tutti i servizi elencati nel presente capitolo sono previsti come necessari nelle modalità di erogazione dei servizi infrastrutturali oggetto del presente documento.



TIM - Uso Interno - Tutti i diritti riservati.

### 4.2.1 Componente Data Center Interconnection

#### 4.2.1.1 *Il Backbone IP/MPLS*

Le due Region saranno collegate da una rete IP su un backbone **proprietario** IP/MPLS (nx100GBE) impiegando solamente apparati router carrier class. La topologia di rete sarà di tipo "Hub and Spoke" in cui gli spoke, i DC, sono collegati in modalità "Dual Homing" agli hub, i POP Centro Servizi. Il "Dual Homing" è reso ancora più affidabile attraverso un POP Centro Servizi fisicamente costruito su due centrali differenti. Gli hub sono collegati fra di loro, almeno nel primo rilascio, secondo una topologia partial mesh. Questa topologia garantirà sulla direttrice che collega le due Region il minimo valore di round trip delay (RTT). Tale backbone consentirà inoltre la configurazione di connettività L2 extension tra ciascun DC.

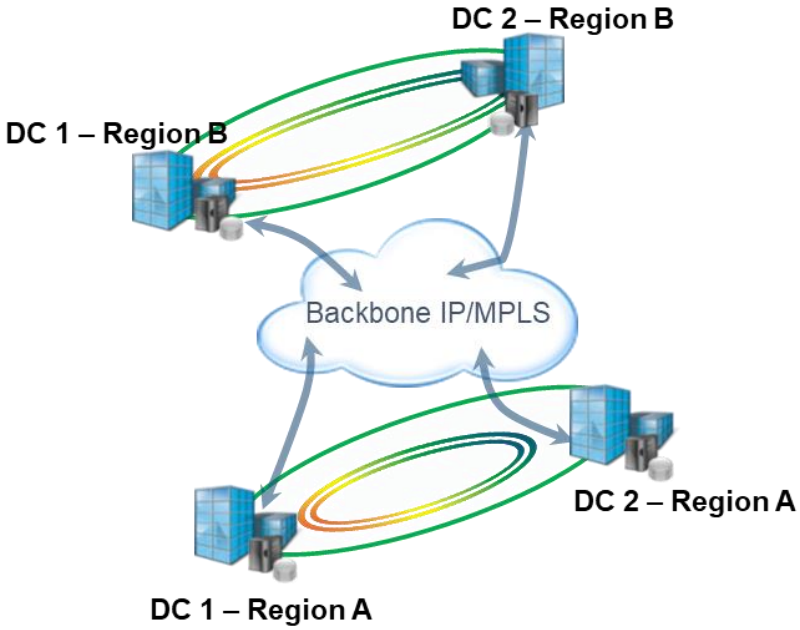



**Figura 17: Connessione Data Center**

Le interconnessioni tra i due Data Center della stessa Region sono realizzate attraverso percorsi indipendenti garantendo una differenza sulla lunghezza di cavo posato non superiore al 20% rispetto al cavo con lunghezza superiore.

#### 4.2.1.2 *Interfaccia Dense Wavelength Division Multiplexing*

Le componenti di Data Center Interconnection prevedono un'interfaccia Dense Wavelength Division Multiplexing (DWDM) **dedicata con traffico cifrato su suolo pubblico**. I Data Center sono interconnessi tra di loro, allo scopo di realizzare un unico campus, attraverso una coppia di collegamenti metropolitani a 100 GBE dedicati.

#### 4.2.1.3 *Virtual Local Area Network*

Le VLAN sono trasportate in ciascun Data Center e all'interno della stessa Region grazie alla tecnologia VXLAN che estende i limiti delle VLAN, mantenendo la separazione dei contesti di ciascun cliente. I Data Center sono interconnessi attraverso una coppia di collegamenti metropolitani a 100 GBE dedicati.



TIM - Uso Interno - Tutti i diritti riservati.

#### 4.2.1.4 *Traffico*

I Data Center saranno realizzati con delle fabric L3 con topologia spine-leaf. Sia il traffico L2 in tunnelling VXLAN sia il traffico L3 routed è veicolato nativamente all'interno di ciascun campus/DC e viene cifrato su ogni matrice di traffico (potendone anche configurare end to end le singole tratte). Questo modello di interconnessione di fatto consente di avere una completa configurazione di interconnessione full mesh (con encryption) tra tutti i singoli DC costituenti i due differenti campus (region).

### 4.2.2 Componente Wide Area Network

La componente di Wide Area Network dovrà prevedere la disponibilità della **connessione Internet condivisa con gli altri servizi Data Center su reti condivise e con doppio upsteam provider**:

- Servizio di DDOS Protection condiviso;
- Intrusion Detection System condiviso: possibilità di eseguire servizi di tipo Intrusion Detection per il traffico cliente e ricevere/gestire allarmi tramite SOC
- Annuncio reti internet da entrambi i DC in modalità indifferenziata (Active/Active)

#### 4.2.2.1 *Internet/Infranet Condivisa*

Il backbone IP/MPLS offre connettività Internet e Infranet (SPC Connettività) effettuando peering diretto con il backbone nazionale attraverso tre POP centro Servizi: NORD, Centro NORD e Centro SUD. I POP Centri Servizi sono collocati per questione di affidabilità presso due Centrali Dati e sono ridondati; di conseguenza i punti di peering sono ben sei, ed è impiegata una logica di prossimità geografica che, allo scopo di minimizzare il delay, costringe a due i punti di ingresso/uscita.
Sui GW di peering del backbone nazionale è realizzato l'immediato rilancio verso la QXN (Servizi di Connettività SPC).
La banda condivisa che sarà messa a disposizione delle amministrazioni contraenti è di 10Gb.

#### 4.2.2.2 *Profilatori di Traffico (Bandwindth management)*

In linea agli apparati di DDoS protection, saranno inseriti dei profilatori di traffico. L'obiettivo è quello di realizzare una piattaforma tecnologica dedicata alla profilazione del traffico afferente a e proveniente dai DC interconnessi alla rete di backbone. Il profilatore di traffico offre la possibilità di creare delle Classi di Servizio per ciascun cliente e offre la possibilità di processare i pacchetti transitanti dai segmenti interessati consentendo di poter effettuare una serie di operazioni richieste dal cliente in fase di stesura dei requisiti tra cui:

- Operazioni di Traffic Classification e Traffic Shaping;
- Decision Marking;
- Policy Enforcement.



TIM - Uso Interno - Tutti i diritti riservati.

Il sistema di gestione QoS consente di creare policy gerarchiche multilivello per utente/gruppi di utenti, servizi, encapsulation (GRE, VLAN), Time of day, DSPC applicando azioni di

- Shaping: possibilità di stabilire una banda massima, banda minima garantita, Priorità, garantendo così l'utilizzo massimale della banda e politiche di "fair usage" tra utenti;
- block/alert /bypass;
- expedite forwarding: consente inoltro rapido dei pacchetti per protocolli sensibili a Jitter;
- steering: la piattaforma supporta deviazione/mirror del traffico in tempo reale verso applicazioni di terze parti;
- http redirection.

Gli apparati saranno completamente trasparenti alla rete, non andando a modificare nulla nei pacchetti che transitano sui link attestati. Inoltre, per preservare la connettività anche in caso di guasto, gli apparati sono dotati di un bypass passivo che permetterà in ogni caso il transito del traffico di rete.

Inoltre saranno applicabili meccanismi Deep Packet Inspection (DPI), che consentono il riconoscimento di un elevato numero di applicazioni e la classificazione della maggior parte del traffico presente sulla rete. Il motore DPI contiene una libreria completa di "signatures" per il riconoscimento di ciascun protocollo/applicazione, nonchè la possibilità di creare "signatures" personalizzate. La libreria delle firme viene aggiornata continuativamente tramite i pacchetti di protocollo pack; gli aggiornamenti sono automatizzati.

#### 4.2.2.3 *IDS e APM*

Ciascun Data Center sarà equipaggiato con Network Packet Broker (NPB). Tali apparati permettono di prelevare il traffico tra gli apparati di rete presso il DC (i FW oppure i LB piuttosto che i Router di Edge dedicati) sia in modalità Online sia in Mirroring e quindi di monitorare lo stesso in tempo reale. I NPB, pertanto, sono dotati di porte in "Bypass" attraverso le quali mettono in comunicazione gli apparati di rete e di porte "Tool" attraverso le quali inviano il traffico prelevato agli apparati di monitoraggio siano essi passivi (APM, IDS) o attivi (IPS) dedicati.

#### 4.2.2.4 *Raccolta linee*

I DC messi a disposizione della PA da parte del PSN saranno collegati sia ad Internet sia alla rete SPC, il che consentirà alle Amministrazioni contraenti di ***usufruire dei servizi senza soluzione di continuità.***

#### 4.2.2.5 *Virtual Private Network*

Su base progetto sarà data la possibilità alle PA di realizzare la soluzione VPN ipsec per la crittografia end to end:

- **VPN IPSEC dedicata su infrastruttura dedicata.** Gestione VPN internet con terze parti con la possibilità di gestire piani di indirizzamento in overlap, attraverso la presenza di



TIM - Uso Interno - Tutti i diritti riservati.

terminatori IPSEC fisici o virtuali dedicati in grado di instaurare una VPN IPSEC e di gestire piani di indirizzamento remoti in overlap con quelli in uso.

- **VPN remote access.** Gestione accessi remoti VPN client con terminazione TLS, con la possibilità di gestire e configurare accessi al DC in modalità client e clientless (https) sicura.

#### 4.2.2.6 *Connettività dedicata per la migrazione dati*

Come servizio opzionale, la NewCo PSN offre la possibilità alle PA che ne faranno richiesta, di fruire di connettività dedicata a partire da 1 Gbps su protocollo gigabit ethernet attraverso la quale è possibile realizzare l'accesso alla rete geografica per i servizi necessari alla migrazione dei dati.
I servizi ad alta velocità prevedono l'utilizzo di infrastrutture in fibra dedicata per collegare la sede del cliente con i punti di accesso al servizio gestito dalla NewCo PSN fino al Data Center di destinazione. L'offerta è caratterizzata da:

**- elevate prestazioni (sia in termini di picco che di banda garantita);**
**- affidabilità;**
**- sicurezza**.

Obiettivo fondamentale è quello di proporre un servizio ai massimi livelli di eccellenza in termini di profilo di servizio, di competenza, supporto tecnico e gestione operativa.L'offerta prevede un servizio di Virtual LAN a livello metropolitano tra le sedi del cliente e il DC con velocità di 1Gbps su protocollo Gigabit Ethernet e la realizzazione di una Rete Privata Virtuale "Globale" (VPN IP), in ambito geografico. L'implementazione delle VPN IP utilizza la tecnologia MPLS, basata sull'instradamento dei pacchetti mediante l'inoltro di etichette ad essi associate (Label Swapping). MPLS non utilizza dunque indirizzi IP pubblici, risultando in questo modo inattaccabile dall'esterno e sicura al pari di una rete ATM/FR e flessibile come una rete IP.
Il servizio prevede la fornitura in sede cliente dell'apparato (Terminazione di rete) installato e gestito da personale della NewCo PSN. In caso di connettività richiesta superiore a 1 Gbps, sono previste le bande a 2 Gbps, 5Gbps e 10 Gbps; per queste bande, per le quali sarà necessaria una proposizione a progetto, l'accesso fisico è realizzato su Lambda Wave (fibra ottica DWDM); per tali reti, i parametri di jitter e packet loss sono trascurabili, mentre la latenza varia in base alla lunghezza delle tratte in fibra e al numero di apparati di rete attraversati. In questo caso, la fibra ottica prevista, l'interfaccia di rete e la capacità di inoltro della CPE consentono di effettuare eventuali upgrade di banda rispetto alla scelta iniziale (dunque da 2Gbps fino a 10 Gbps) senza dover apportare modifiche alle configurazioni hardware ma solo attraverso una riconfigurazione logica.

#### 4.2.2.7 *Hosting del router di terminazione*

Nel caso in cui la PA disponesse di un proprio collegamento geografico dedicato (MPLS), è prevista la possibilità di un hosting della terminazione (router) presso i locali DC in prossimità della sala sistemi.
Questo servizio prevede la disponibilità di spazio fisico in un rack adibito allo scopo e con le seguenti caratteristiche:

- Facilities strutturate;
- Cablaggio strutturato in fibra verso la sala TLC;
- Cablaggio in rame verso la DMZ che ospita i gateway dei sistemi Cliente;



TIM - Uso Interno - Tutti i diritti riservati.

- Attività di configurazione della LAN di raccordo tra i gateway Cliente e la terminazione geografica.

La soluzione richiede una verifica propedeutica di posizionamento dell'apparato e utilizzo di bretelle di collegamento.

### 4.2.3 Componente Local Area Network

I Data Center prevedono la disponibilità dei seguenti apparati in merito alla componente Local Area Network (LAN).

#### 4.2.3.1 *Apparati condivisi (locali in DC o estesi sui due DC)*

Di seguito l'elenco degli apparati dedicati previsti per l'erogazione dei servizi oggetto del presente Progetto di Fattibilità, tutti costantemente monitorati:

- **FIREWALL** segregazione della rete
  - DMZ dedicata su interfacce condivise 1 Gbs: DMZ logica (vlan) dedicata su firewall condiviso con interfacce 1 Gbs;
  - DMZ dedicata su interfacce condivise 10 Gbs: DMZ logica (vlan) dedicata su firewall condiviso con interfacce 10 Gbs.
- **APPLICATION DELIVERY CONTROL:**
  - Servizio di bilanciamento e terminazione sessioni TLS con gestione certificato: virtual server logico dedicato su bilanciatore condiviso con altri servizi/clienti.
  - Web Application Firewall: policy WAF dedicate ed agganciate a virtual server logico, tramite licenza Application Security Manager su bilanciatore condiviso.
  - Autenticazione, SSO, CRL: configurazione Application Policy Manager su virtual server logico dedicato su bilanciatore condiviso.
- **ROUTER**
  - Tabella di routing dedicata su dominio routing condiviso: VRF dedicata su infrastruttura di Data Center condivisa.
- **SWITCH**
  - Broadcast domain dedicato su dominio di switching condiviso: VLAN dedicata su infrastruttura di Data Center condivisa. Gli switch utilizzati e proposti nel ruolo di LEAF per la raccolta della connettività esterna (internet/infranet), verso la farm, piuttosto che gli apparati L4/L7, sono equipaggiati:
  - per la raccolta in fibra con 48 x 1/10/25-Gbps fiber ports (lato host) e 6 x 40/100-Gbps (lato spine);
  - per la raccolta in rame con 48 x 100M/1/10GBASE-T ports (lato host) e 6 x 40/100-Gbps (lato spine);
  - gli switch utilizzati e proposti nel ruolo di SPINE, sono apparati modulari carrier-class equipaggiati con porte 100 GBE.



TIM - Uso Interno - Tutti i diritti riservati.

- **DNS**
  - Gestione entry su dominio dedicato ai servizi della NewCo: setup entry dedicate su zona gestita tramite DNS autoritativi.
- **NAC area uffici e area housing**
  - Gestione di un'area di Office tramite accessi su switch completamente dedicati e separati da quelli di Datacenter. Gli switch di ufficio eseguiranno autenticazione 802.1x colloquiando con un radius (infranet controller) e con autenticazione finale dell'utente in modalità Two Factor demandata ad un server ldap centralizzato. I laptop autorizzati avranno un client installato in grado di colloquiare in 802.1x ed in maniera centralizzata saranno controllate le caratteristiche del client (host checker) che dovrà soddisfare i requisiti minimi di sicurezza (es. allineamento antivirus, etc)
  - Gestione dell'area housing tramite accessi su switch che eseguiranno autenticazione 802.1x colloquiando con un radius (infranet controller). Tale soluzione può essere esclusa se le misure di sicurezza fisica permettono di garantire un adeguato need-to-access alle reti

#### 4.2.3.2 *Apparati dedicati (locali in DC o estesi sui due DC)*

Su base progetto verranno resi disponibili i seguenti apparati:

- **FIREWALL**
  - Firewall L4 interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs.
  - Firewall L4 interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs.
  - Firewall UTM interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs e licenza UTM.
  - Firewall UTM interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs e licenza UTM.
  - Firewall NGFW interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs e licenza NGFW.
  - Firewall NGFW interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs e licenza NGFW.

La gestione unificata degli attacchi, comunemente abbreviata in UTM, è un termine inerente alla sicurezza informatica, che indica una singola soluzione e, una singola applicazione di protezione che offre più funzioni di sicurezza in un unico punto della rete. Un'applicazione UTM include, normalmente, funzioni come: antivirus, anti-spyware, anti-spam, firewall di rete, rilevamento e prevenzione delle intrusioni, filtraggio dei contenuti e protezione dalle perdite di dati. Tutte queste applicazioni (application filtering, IPS, AntiVirus, Web Filtering, Domain Reputation AntiSpam etc), sono disponibili sui dispositivi FW proposti.

- **APPLICATION DELIVERY CONTROL**



TIM - Uso Interno - Tutti i diritti riservati.

- Servizio di bilanciamento e terminazione sessioni TLS con gestione certificato: bilanciatore appliance.
- Web Application Firewall: licenza Application Security Manager su bilanciatore appliance.
- Autenticazione, SSO, CRL: licenza Application Policy Manager su bilanciatore appliance.
-

- **SWITCH**
  - Switch interfacce 1 Gbs: switch con interfacce ad 1 Gbs.
  - Switch interfacce sino 10 Gbs: switch con interfacce sino a 10 Gbs (sfp).
- **DNS**
  - Gestione zona dedicata: gestione della zona del cliente su DNS autoritativi internet.
- **NAC**
  - Gestione dell'accesso dei client autorizzati ad un'area Office.

## 4.3 Facility

I Servizi di Facility consistono nella messa a disposizione, da parte della NewCo PSN, di aree all'interno dei Data Center, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti:

- Spazi attrezzati;
- Sistemi HVAC;
- Sicurezza Fisica;
- Rack e Cage.

Il dettaglio dei servizi è descritto nel ***capitolo 5 – Caratteristiche Data Center***.
La NewCo PSN si farà carico di tutte le attività di progettazione e set up delle Facilities, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

### 4.3.1 Energia Elettrica

Il Servizio prevede la Fornitura dell'energia elettrica necessaria all'alimentazione delle infrastrutture descritte nel presente Progetto di fattibilità.

La NewCo PSN fornirà ad ogni PA con cadenza mensile, un report afferente i consumi elettrici relativi alle infrastrutture oggetto del Servizio, riportante:

- La potenza elettrica complessivamente assorbita nel mese precedente (espressa in kW) relativa a ciascun rack e derivante dall'insieme di apparati IT e TLC presenti



TIM - Uso Interno - Tutti i diritti riservati.

- La potenza elettrica complessivamente assorbita nel mese precedente (carico IT, espressa in kW) quale sommatoria delle potenze elettriche assorbite dalla totalità dei rack (kWIT)

Il prezzo dell'energia elettrica è composto da alcune componenti variabili nel tempo e non controllabili dalla NewCo PSN, quali:

- PUNIndex: è la media aritmetica mensile, espressa in Euro/kWh e arrotondata alla seconda cifra decimale, dei valori orari del PUN (), rilevati sulla piattaforma telematica: Mercato Elettrico – Mercato Elettrico a pronti (MPE) – Mercato del Giorno Prima (MGP). Tale quotazione, al momento di pubblicazione del presente bando, risulta pubblicata sul sito internet del GME tra i dati di sintesi MPE-MGP – riepilogo; colonna media dei Prezzi d'acquisto, PUNIndex (€/kWh) della sintesi mensile, nella sezione Esiti dei mercati e statistiche – Statistiche;
- Oneri: oneri di sistema del solo Mercato Libero (a titolo esemplificativo le componenti tariffarie A, UC, MCT), come stabiliti, volta per volta, dall'AEEGSI (www.autorita.energia.it). Relativamente algi oneri verrà riconosciuta alla NewCo PSN esclusivamente delle tariffe la parte variabile (solo la quota addebitabile al cliente finale espressa in €/kWh)
- Dispacciamento: corrispettivi relativi alle componenti che costituiscono i costi per il dispacciamento sul mercato libero (le cui componenti sono pubblicate da TERNA e dall'AEEGSI);
- Perdite di Rete: prezzi unitari dovuti per le perdite di energia elettrica dati dal prodotto dei fattori percentuali di perdita di energia elettrica sulle reti con l'obbligo di connessione di terzi così come definite nella colonna (A) della Tabella 4 del TIS e delle voci "PUNIndex" e "Dispacciamento" precedentemente definite;
- Trasporto: oneri di Trasmissione, Distribuzione e Misura, così come stabiliti, volta per volta, dall'AEEGSI. Relativamente al trasporto verrà riconosciuta alla NewCo PSN esclusivamente delle tariffe la parte variabile (solo la quota addebitabile al cliente finale espressa in €/kWh)
- Fiscalità: tassazione prevista dalla normativa vigente relativa alla fornitura di energia elettrica al netto della sola IVA.

Essendo le componenti sopra descritte variabili nel tempo e non controllabili dalla NewCo PSN, sarà previsto durante l'esecuzione del contratto un meccanismo di aggiornamento delle tariffe esposte, con cadenza trimestrale su base mensile.



TIM - Uso Interno - Tutti i diritti riservati.

# 5 Caratteristiche Data Center

I siti saranno localizzati in un'area servita da connettività SPC, i cui tre fornitori di riferimento sono stati selezionati nell'ambito della Gare per l'affidamento dei servizi di connettività (ID Sigef 1367), la cui composizione è stata pubblicata il 15/06/2016 sul sito dell'Agenzia per l'Italia Digitale.

Saranno rispettate tutte le disposizioni attualmente vigenti relative alle infrastrutture di Information Technology, quali:

- Requisiti indicati dal D.Lgs. 81/2008 Testo Unico sulla salute e sicurezza sul lavoro;
- Cavi UTP rispondenti a ISO/IEC 11801 almeno categoria 5;

## 5.1 Determinazione caratteristiche del macrosistema Data Center

**Caratteristiche dei Data Center**

La NewCo PSN prevede di impiegare **n.4 Data Center** aventi caratteristiche aderenti allo **standard ANSI/TIA 942**, coerentemente con quanto indicato da AgID nelle "*Linee guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione*", pubblicate sul sito dell'Agenzia (https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lg_razionalizzazione_ced_pa_0.pdf)

aventi le specifiche di seguito riportate:

- I 4 Data Center saranno allestiti in doppia Region (2 DC + 2 DC), la singola Region avrà i due diversi Data Center distanti almeno 5 Km in linea d'aria e non più di 60 Km di distanza in fibra in doppio percorso completamente distinto fra l'uno e l'altro, evitando così di avere un singole point of failure (SPOF); posizionati ad una distanza adeguata all'erogazione di servizi Active-Active Geografico. La latenza garantita è definita nei capitoli relativi alle caratteristiche di connessione;
- Le due Region saranno geograficamente posizionate ad una distanza tale da consentire la realizzazione di tutti i servizi di Disaster Recovery in maniera efficace. Nello specifico esse saranno ubicate ad una distanza **minima di 500 Km** all'interno del territorio nazionale in aree con condizioni di rischio diverse tra loro. Nelle valutazioni di rischio considerate si citano, a titolo indicativo ma non esaustivo:
    - Rischio sismico;
    - Rischio idrogeologico;
    - Rischio ambientale;
    - Rischio terroristico;
    - Rischio inquinamento ambientale e/o industriale
- La soluzione proposta prevede di utilizzare in una prima fase 2 Data Center con le seguenti caratteristiche:
    - un Data Center di una delle due Region in possesso delle seguenti certificazioni:



TIM - Uso Interno - Tutti i diritti riservati.

- **UPTIME INSTITUTE Tier IV Constructed Facilities;**
- **ANSI TIA 942 Rating 4**;
- EN 50600 classe 4;
- ISO 27001;
- ISO 14001.

  - un Data Center di una delle due Region in possesso delle seguenti certificazioni:
    - **UPTIME INSTITUTE Tier IV Design Facilities;**
    - entro 3 mesi dalla sottoscrizione della convenzione certificazione **UPTIME INSTITUTE Tier IV Constructed Facilities;**
  - I 2 ulteriori Data Center in possesso della certificazione **Uptime Institute Tier III Design Facilities e ANSI TIA 942 Rating 3**.

- In una seconda fase si avrà:
  - Entro 21 mesi dalla sottoscrizione della Convenzione, 2 DC certificati **UPTIME INSTITUTE Tier IV Constructed Facilities**;

**La configurazione finale prevede l'utilizzo di 4 DC, su due region, tutti certificati sia UPTIME INSTITUTE Tier IV Constructed Facilities sia ANSI/TIA 942 Rating 4.**

- Entro 18 mesi dalla sottoscrizione della Convenzione, la NewCo PSN avrà almeno una Region in possesso della certificazione **LEED Gold (cfr. §.5.2.3.1)**.
- Per ognuno dei 4 DC coinvolti nel progetto saranno dedicati gli spazi utili per alloggiare i rack secondo un modello di incremento modulare nel tempo, in funzione delle adesioni delle PA al PSN. Tale crescita parte da uno spazio iniziale di 800mq con potenza complessiva di 1.150 Kw e può incrementare in maniera modulare fino ad uno spazio complessivo di 2.900mq con una potenza totale di 4.800Kw.

**Caratteristiche della rete dei Data Center e delle Region:**
La topologia di rete di scelta per realizzare ciascun Data Center sarà basata su una architettura Spine-Leaf a 100GBE che utilizza la tecnologia VXLAN per incapsulare i frame layer 2 dentro UDP header con l'obiettivo di estendere il dominio di switching attraverso una rete layer 3 IP. La diffusione delle Informazioni layer 2 (MAC address) e layer 3 (host IP address), affidata al control plane MP-BGP EVPN, rende estremamente scalabile la rete. Una fabric L3 IP inoltre è, per definizione, spanning tree free rendendo la rete più stabile; ha tempi di convergenza molto contenuti (dell'ordine delle decine di msec) e consente in modo semplice ed automatico la distribuzione del traffico tra i vari link e, pertanto, l'utilizzo ottimale delle risorse di rete. IL consumo delle vlan_id è poi ampiamente superato in quanto il VXLAN estende il range delle vlans da 4096 ad oltre 16 milioni. Un altro importante vantaggio di una fabric L3 è la possibilità di attivare il Distributed Gateway che, presentando lo stesso ip address gateway su tutti gli Edge Switch (LEAF), offre ad ogni endpoint la possibilità di essere ruotato localmente nel punto più vicino. Tutti i nodi della fabric sono dual stack, caratteristica fondamentale per introdurre il protocollo ipv6 senza dover ricorrere a tecniche di tunnelling o di NAT che limitano inevitabilmente la scalabilità della rete. Le fabric Spine-Leaf di ciascun Data Center dell'architettura richiesta dovranno esser unite tra di loro attraverso dei collegamenti metropolitani a 100 GBE dedicati. Tuttavia, per superare i limiti di scalabilità delle stretched



TIM - Uso Interno - Tutti i diritti riservati.

fabric, sono impiegati dei nodi L3, che da un lato sono collegati agli spine locali e d'altro terminano i collegamenti di DCI metropolitani con la controparte dell'altro Data Center. La topologia di rete che risulta si chiama Multi POD.

I Data Center utilizzati adotteranno la tecnologia SDN (software defined networking) per il controllo centralizzato e automatizzato di tutti i processi, dal deploy di una nuova applicazione alla relativa manutenzione e monitoraggio. In particolare, **i due Data Center di ciascuna Region saranno gestiti da un unico controller SDN** che, per ragioni di alta affidabilità, sarà costituito da un cluster di server distribuiti tra le due fabric. La Region può essere pertanto considerata come un unico campus, caratterizzato da un unico dominio VXLAN che rende l'estensione L2 tra i due Data Center come qualcosa di intrinsecamente sempre valido e garantito senza dover intervenire in alcun modo sui collegamenti che realizzano il DC Interconnection. Sfruttando il controller SDN, si realizzerà una architettura multisite tra le due Region, realizzando un vero e proprio Campus geografico, non solo per estendere e mettere a fattor comune risorse tra le due Region ma anche per scopi di disaster recovery.

### 5.1.1 Caratteristiche geografiche e topografiche

I Data Center saranno posizionati in aree di rischio sismico classificate come zona non inferiore alla zona 3 secondo il DM 58 del 2017. Per quanto attiene al rischio idrogeologico, le strutture sono presenti in aree a basso rischio. Nel caso in cui l'area presenti potenziali rischi, sarà data evidenza di tutte le azioni correttive adottate al fine di gestire e superare le eventuali criticità.

Dal punto di vista dei rischi ambientali ed esterni si manifesta la preferenza per siti aventi le seguenti caratteristiche intrinseche:

- Lontananza significativa da vie costiere o vie navigabili interne;
- Lontananza dalle principali arterie di traffico;
- Vicinanza alle grandi aree metropolitane;
- Distanza inferiore o uguale a 10 km e uguale o non superiore a 50 km rispetto ad aeroporti.

### 5.1.2 Indipendenza connessioni elettriche ed impiantistiche

Le infrastrutture tecnologiche dei Data Center non avranno punti di alimentazione esterna comune.

Al fine di meglio chiarire l'affermazione, non sono utilizzati Data Center alimentati dalla medesima sottostazione di alta tensione e/o derivati dalla stessa rete urbana di media tensione.

## 5.2 Determinazione caratteristiche dei singoli Data Center

### 5.2.1 Caratteristiche dimensionali del sito

Di seguito si riportano le caratteristiche dimensionali target che saranno rese disponibili per ogni sito:



TIM - Uso Interno - Tutti i diritti riservati.

- Spazio netto data-room disponibile: ognuno dei 4 DC coinvolti nel progetto metterà a disposizione gli spazi dedicati utili per alloggiare i rack secondo un modello di incremento modulare nel tempo, in funzione delle adesioni delle PA al PSN. Tale crescita parte da uno spazio iniziale che varia da 100 mq a 350 mq e può incrementare in maniera modulare fino ad uno spazio complessivo che varia da 250 mq a 700 mq.
- Potenza IT disponibile: non inferiore a 1.150 KW totale al tempo T0.
- Numero rack da ospitare: non inferiore a 100 complessivi al tempo T0, riproporzionati sulla base dei mq dei singoli siti.

### 5.2.2 Caratteristiche topografiche ed ambientali

La configurazione topografica del datacenter, oltre alle sale informatiche ad uso esclusivo richieste al punto precedente, garantirà anche la presenza dei seguenti spazi e/o servizi accessori:

- Magazzino a temperatura controllata con spazio segregato dedicato non inferiore ai 50 mq;
- Disponibilità di "TEST AREA" ad uso condiviso per la prova e test delle apparecchiature informatiche prima dell'installazione in dataroom;
- Aree condivise di smart working per tecnici e specialisti;
- Baia di carico/scarico merci, con percorso dedicato ed indipendente dal percorso pedonale. Tale area sarà monitorata e controllata dal sistema di vigilanza.

### 5.2.3 Caratteristiche architettoniche e strutturali

Di seguito si riportano le caratteristiche architetturali e strutturali target che saranno rese disponibili per ogni sito:

- Portata pavimenti non inferiore a 800 kg/mq
- RACK da 42, 48, 52
- Vie di accesso garantite alle dataroom non inferiori a 1200 x 2100 mm netti;

#### 5.2.3.1 *Sostenibilità energetica e certificazioni*

I Data Center sono gestiti nel segno dell'efficienza energetica e della sostenibilità ambientale; la NewCo PSN adotta politiche e modelli produttivi che riducono al minimo le emissioni e limitano l'utilizzo delle risorse ambientali.




La NewCo si doterà di edifici costruiti e gestiti secondo principi "green", ovvero prevedendo le più avanzate tecniche di raffreddamento, ma anche soffitti e mura in grado di gestire al meglio la temperatura, l'impiego di batterie agli ioni di litio al posto di quelle al piombo, di luci LED a basso consumo energetico, impianti fotovoltaici che contribuiscono al contenimento del PUE.



TIM - Uso Interno - Tutti i diritti riservati.

Vengono utilizzati dispersori geotermici ad una profondità di 30 mt per lo smaltimento del calore prodotto dai Gruppi Frigo, raddoppiando così il rendimento degli stessi.
In alcuni Data Center si utilizzano D-UPS (UPS dinamici) che non hanno bisogno dell'utilizzo delle batterie andando così ad aumentare la sostenibilità ambientale.
Gli apparati più datati, che richiedono un maggiore consumo di energia, vengono costantemente sostituiti con apparati nuovi e in grado di beneficiare di soluzioni più efficienti, come l'EPV (Evaporative Free Cooling), che permettono di ridurre i costi e di garantire una maggiore resilienza operativa.

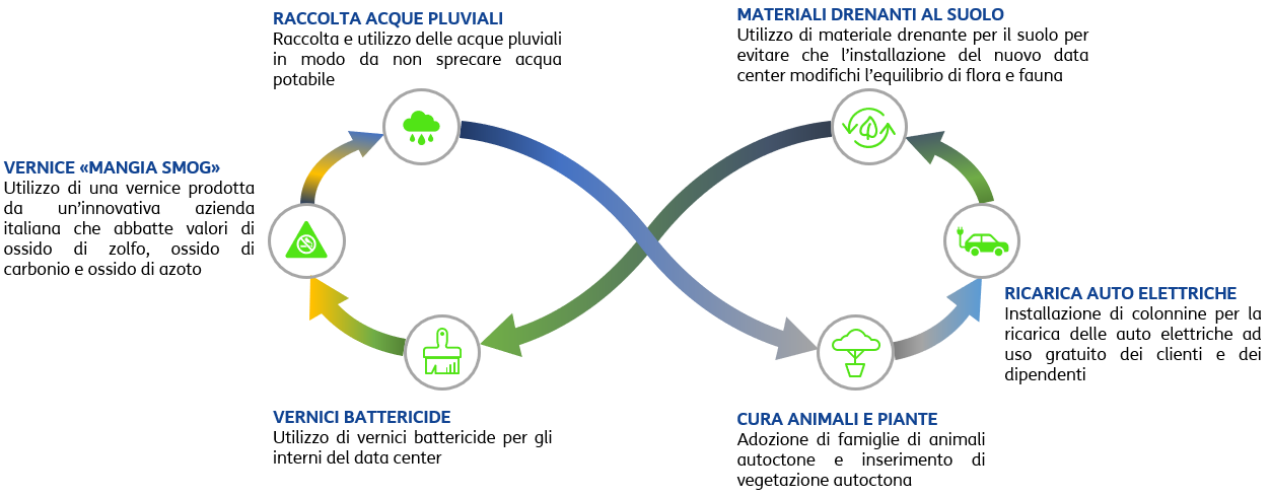



**Figura 18: Ciclo virtuoso energia dei Data Center**

Per quanto riguarda il footprint ambientale, i DC hanno fissato l'obiettivo di raggiungere il livello di PUE inferiore 1,4 e diventare carbon neutral entro il 2030.

I Data center della NewCo PSN potranno inoltre vantare le seguenti certificazioni:

**Certificazione ISO 50001**
Per le aree che hanno un impatto rilevante sulla Comunità, attraverso prodotti e servizi offerti, i Data Center impiegati dall NewCo PSN hanno ottenuto le certificazioni che assicurano l'adozione di procedure e comportamenti in linea con le aspettative degli stakeholder. In particolare, la norma ISO 50001 è la certificazione relativa a requisiti per creare, avviare, mantenere e migliorare un sistema di gestione dell'energia ed ottimizzare in modo continuo la propria prestazione energetica.
La norma definisce i requisiti applicabili all'uso e consumo dell'energia, includendo l'attività di:

- misurazione,
- documentazione,
- progettazione,
- acquisto per le attrezzature,

nonché i processi e il personale che contribuiscono a determinare la prestazione energetica.

**Certificazione ISO 14001**
I Data Center impiegati dalla NewCo PSN possono vantare la certificazione ISO 14001 che è la norma di riferimento per le aziende dotate di un Sistema di Gestione Ambientale. I requisiti



TIM - Uso Interno - Tutti i diritti riservati.

prevedono che il "Sistema di gestione Ambientale" sia parte integrante del sistema di gestione aziendale e sia volto a gestire gli aspetti ambientali, soddisfare gli obblighi di conformità legislativa e affrontare e valutare i rischi e le opportunità.

**Certificazione LEED**

La certificazione costituisce una verifica di parte terza, indipendente, delle performance dell'intero edificio sede del Data Center. La certificazione LEED, riconosciuta a livello internazionale, afferma che un edificio è rispettoso dell'ambiente e che costituisce un luogo salubre in cui vivere e lavorare. L'ottenimento della certificazione LEED permette di ottenere sia vantaggi economici che ambientali, tra cui:

- stabilire uno standard comune di misurazione dei "green buildings", definiti come edifici a basso impatto ambientale;
- fornire e promuovere un sistema di integrato di progettazione che riguarda l'intero edificio;
- la riduzione dei rifiuti inviati in discarica, esempio di economia circolare;
- i risparmi energetico e idrico, utilizzando free-cooling e la gestione delle acque meteoriche;
- lo sviluppo di edifici più sani e più sicuri, abolendo il fumo e garantendo la qualità dell'aria;
- la creazione di comunità compatte e accessibili, con buon accesso ai servizi di vicinato e di transito;
- la tutela delle risorse naturali, incoraggiando lo sviluppo urbano in zone già antropizzate;
- la riduzione delle emissioni nocive di gas serra, utilizzando gas non nocivi.

## 5.2.4 Infrastruttura elettrica

### 5.2.4.1 *Impianto di terra e protezione scariche atmosferiche*

L'intero insediamento sarà attrezzato con un impianto di terra adeguatamente dimensionato e realizzato in accordo alle norme vigenti.
All'impianto di terra faranno capo:

- Impianto di protezione elettrica;
- Impianto di equalizzazione del potenziale realizzato all'interno dell'insediamento e nelle dataroom a servizio degli armadi racks;
- Impianto di terra "pulita" informatica necessaria ad alcuni apparati IT;
- Impianto di protezione scariche atmosferiche.

L'intero Data Center sarà protetto da impianto di protezione dalle scariche atmosferiche. Saranno altresì protetti da impianto di captazione tutti i manufatti e le apparecchiature inerenti al Data Center posizionati all'esterno.



TIM - Uso Interno - Tutti i diritti riservati.

#### 5.2.4.2 *Stazione di energia normale*

Per i siti certificati Rating 4 e TIER IV l'insediamento sarà alimentato da non meno di due cabine elettriche di trasformazione tra loro indipendenti e segregate da compartimenti antincendio REI120. Ogni cabina apparterrà ad un ramo di alimentazione del Data Center e sarà dimensionata e certificata per garantire l'alimentazione di tutto l'insediamento in caso di down del secondo ramo (configurazione 2N).

#### 5.2.4.3 *Stazione gruppi elettrogeni di emergenza*

L'alimentazione del Data Center sarà garantita in caso di down dell'ente erogatore da stazioni di energia in configurazione minima N+1. I gruppi elettrogeni potranno essere in bassa o media tensione in funzione delle potenze nominali in gioco.

Le macchine saranno dotate di serbatoio combustibile giornaliero a bordo macchina e serbatoio di stoccaggio. Il sistema garantirà una autonomia di funzionamento alla potenza nominale senza rabbocco di carburante non inferiore a 48 ore nelle condizioni di perdita di una sorgente di emergenza per qualsiasi causa o guasto.

#### 5.2.4.4 *Stazione UPS di continuità servizio*

La continuità elettrica sarà garantita da non meno di 2 isole di continuità assoluta (una per ogni ramo di alimentazione) e saranno utilizzate per l'alimentazione del carico IT in configurazione 2N.

Sarà garantita una autonomia minima di 20 minuti a carico nominale certificato con batterie stazionarie alle condizioni di fine vita.

In caso di utilizzo di gruppi statici di continuità di tipo dinamico l'inerzia meccanica dovrà garantire l'alimentazione del carico nominale per non meno di 40 secondi.
I gruppi di continuità saranno alloggiati in locali dedicati e compartimentati rispetto agli altri locali tecnici.

Le batterie saranno installate in locali tecnici ad esse dedicati, compartimentati tra loro e verso gli altri locali. Saranno inoltre dotati di sistema di ventilazione forzata e sensori di rilevazione della presenza di idrogeno. Le batterie dei gruppi di continuità saranno monitorate da un impianto di controllo e verifica dello stato delle batterie per analizzare lo stato di esercizio delle stesse nelle condizioni ordinarie di funzionamento ed in condizioni di scarica e ricarica.

#### 5.2.4.5 *Sistema pulsanti di sgancio di emergenza*

Il Data Center sarà dotato di un impianto di sganci di emergenza realizzato in accordo con le richieste di prevenzione incendi. Gli impianti dovranno comunque rispettare le seguenti precauzioni minime:

- Sarà realizzato un quadro di sgancio di emergenza per ogni ramo di distribuzione elettrica. I quadri saranno installati in locali differenti e compartimentati tra loro. I cavi saranno posati in canalizzazioni dedicate ed identificate solo per tale scopo e viaggeranno in compartimentazioni antincendio separate.
- Dovranno essere predisposti pulsanti di sgancio differenti per i vari servizio:



TIM - Uso Interno - Tutti i diritti riservati.

- Sgancio energia normale;
- Sgancio sorgenti di emergenza (possibilmente con sganci singoli per ogni gruppo elettrogeno);
    - Sgancio sorgenti in continuità assoluta (uno sgancio per ogni isola e/o per ogni gruppo di continuità assoluta).

#### 5.2.4.6 *Rete di distribuzione primaria e secondaria*

La distribuzione elettrica primaria e secondaria sarà realizzata mediante distribuzione in cavo su passerelle e/o con l'utilizzo di condotti sbarra prefabbricati.

All'interno delle sale informatiche, così come nelle altre aree del Data Center, la distribuzione primaria (dalle cabine elettriche ai quadri di zona) e la distribuzione secondaria (dai quadri di zona alle utenze finali) dovranno essere realizzate con canalizzazioni separate ed adeguatamente identificate.

Dovranno inoltre essere garantite le separazioni delle vie cavi relative a servizi diversi. Per tale motivo saranno opportunamente predisposti canalizzazioni differenti per servizi di distribuzione elettrica, impianti ausiliari, impianti di trasmissione dati primaria e secondaria; distribuzione dati in fibra ottica ed in rame ed impianti di sicurezza.

#### 5.2.4.7 *Impianti di illuminazione*

All'interno di tutte le aree del Data Center (sale informatiche e spazi tecnologici) sarà realizzato un impianto di illuminazione atto a garantire l'adeguato livello di illuminazione previsto dalle normative vigenti nelle sale informatiche e nelle aree tecnologiche.

All'interno di ogni locale sarà garantita la presenza dell'illuminazione da sorgenti in continuità assoluta e da sorgente di emergenza (interruzione breve).

Sarà inoltre realizzato un impianto di illuminazione di sicurezza con apparecchi muniti di gruppo autonomo di emergenza (autonomina minima garantita 60 minuti) o con soccorritore centralizzato. Tale impianto garantirà un livello minimo di illuminazione di sicurezza non inferiore ai 5 lux.

#### 5.2.4.8 *Impianti di forza motrice dataroom*

L'infrastruttura elettrica del Data Center garantirà l'alimentazione standard per ogni rack costituita da:

- Presa industriale interbloccata 230V – 32 A - alimentazione di ramo A;
- Presa industriale interbloccata 230V – 32 A - alimentazione di ramo B.

Le singole linee elettriche saranno protette singolarmente da interruttore automatico dedicato. Ogni linea sarà opportunamente monitorata al fine di verificare e controllare gli assorbimenti elettrici ed i consumi energetici. Gli assorbimenti elettrici sono misurati per singolo blindo ovvero per singola fila di rack.



TIM - Uso Interno - Tutti i diritti riservati.

#### 5.2.4.9 *Rete infrastruttura per manutenzione*

Come indicato nelle pagine precedenti la proposta è atta a garantire una infrastruttura elettrica avente caratteristiche tecniche coerenti con il rating TIER III/3 Uptime Institute o ANSI TIA.

Le infrastrutture, coerenti ai requisiti imposti dagli enti sopracitati, prevedono la possibilità/ di effettuare la corretta manutenzione degli apparati e infrastrutture elettriche garantendo l'alimentazione elettrica in continuità assoluta dei quadri di sala (anche dalla stessa sorgente in continuità assoluta) in caso di spegnimento parziale o totale di un ramo di alimentazione e distribuzione o delle apparecchiature elettriche ad esso collegate.

### 5.2.5 Infrastruttura climatizzazione

L'impianto di climatizzazione a servizio del Data Center sarà realizzato al fine di traguardare gli obiettivi del rating TIER III/3 minimi riferiti alle normative di certificazione. L'infrastruttura garantirà infatti la possibilità di eseguire qualsivoglia intervento di manutenzione ordinaria o straordinaria garantendo la continuità di esercizio dell'impianto.

All'interno delle dataroom saranno sempre garantite nei corridoi freddi (corridoi in cui è immessa l'aria di raffreddamento) il mantenimento dei valori termoigrometrici all'interno dei range raccomandati da ASHRAE Thermal Guidelines for Data Processing Environments: 18÷27°C, 20÷80% H.R.Il controllo delle condizioni sopra descritte sarà garantito da sonde di temperatura ed umidità connesse al sistema BMS di monitoraggio. Le sonde saranno installate a circa 1,6 m da quota pavimento e dovranno essere in numero congruo a garantire il monitoraggio completo delle sale.

La climatizzazione dei locali tecnici a servizio del Data Center (cabine elettriche, locali UPS, etc.) sarà garantita da impianti in configurazione 2N. Le temperature di esercizio saranno conformi alle caratteristiche delle apparecchiature installate.
I locali contenenti batterie di accumulatori saranno dotati di sistema di estrazione e ricambio d'aria dedicato avente le caratteristiche conformi all'utilizzo in atmosfere con presenza potenziale di idrogeno.

#### 5.2.5.1 *Stazione di energia termica e frigorifera*

Il Data Center avrà sistemi di produzione di energia frigorifera indipendenti al fine di garantire una configurazione minima N+1.

Ogni sistema sarà dimensionato al fine di garantire il corretto raffreddamento dei carichi di progetto nelle condizioni climatiche più estreme relative al luogo di installazione. Per tale verifica saranno considerati le condizioni climatiche previste dall'ASHRAE HANDBOOK a n=20 anni.

#### 5.2.5.2 *Efficienza Sistema di raffreddamento*

Il sistema di raffreddamento del Data Center ed in particolare delle dataroom sarà realizzato al fine di garantire nelle diverse condizioni di carico IT un'efficacia energetica coerente con un PUE massimo di 1.6. Tale valore dovrà essere calcolato considerando tutti i carichi elettrici a servizio



TIM - Uso Interno - Tutti i diritti riservati.

del Data Center, ivi compresi i carichi luce e forza motrice dei locali e/o spazi di servizio da esso collegati.

#### 5.2.5.3 *Sistema di controllo HVAC*

L'impianto di climatizzazione sarà gestito, controllato e comandato da un impianto di termoregolazione a cui faranno capo anche tutti le sonde posizionate nelle dataroom.

#### 5.2.5.4 *Reti di distribuzione idroniche e / o areauliche*

Le reti di distribuzione provenienti dalle due stazioni di produzione indipendenti saranno tra loro separate e compartimentate ai fini antincendio fino all'ingresso della singola dataroom.
Particolare attenzione sarà posta al fine di evitare la possibilità di ghiacciamento dei fluidi all'interno delle tubazioni e delle apparecchiature in caso di installazioni all'esterno in climi particolarmente rigidi nel periodo invernale.

#### 5.2.5.5 *Rete di adduzione*

In caso di utilizzo di impianti di raffreddamento ad acqua di torre, ovvero impianti con utilizzo di acqua di falda e quindi dipendenza dell'infrastruttura di climatizzazione da sorgenti esterne, sarà garantita la presenza di vasche di accumulo adeguatamente dimensionate al fine di garantire una autonomia nel caso di funzionamento in isola dei sistemi di almeno 12 ore nelle condizioni più estreme.

#### 5.2.5.6 *Rete di scarico acque nere ed acque bianche*

Le reti di scarico del Data Center saranno opportunamente allacciate alle reti municipali al fine di evitare qualsivoglia reflusso in caso di eventi straordinari che impattino sulle reti di smaltimento delle acque meteoriche e reflue.

Nel caso questo rischio sia evidenziato, saranno predisposte e proceduralizzate soluzioni tecniche di emergenza da attivare in casi critici.

### 5.2.6 Impianti ausiliari e protezione incendio

Il Data Center sarà dotato di impianti ausiliari ad alto contenuto tecnologico necessario per la corretta gestione delle infrastrutture, nonché alla riduzione dei rischi di incendio sia per le persone che per le apparecchiature ed i servizi ad esse collegati.

#### 5.2.6.1 *Impianto rivelazione fumi ed antiallagamento*

Tutte le aree del Data Center saranno dotate dei seguenti impianti di rivelazione fumi:

- Impianto VESDA (Very Early Smoke Detection Apparatus). Installato in tutti i locali garantirà una rilevazione precoce di fumo. Non necessariamente entra nelle logiche di comando ed attivazione dei sistemi di spegnimento automatico. È interfacciato con la centrale di rilevazione fumi e/o con il sistema di BMS;
- Impianto rilevazione fumi indirizzato. Installato in tutti i locali secondo le indicazioni della norma UNI9795. Gestisce l'allarme incendio ed è interfacciato con i sistemi di spegnimento



TIM - Uso Interno - Tutti i diritti riservati.

automatico. È caratterizzato da sensori di fumo o calore, pulsanti ad attivazione manuale e segnalatori ottici acustici. Comanda anche tutte le serrande tagliafuoco installate sui canali di ventilazione.

#### 5.2.6.2 *Impianto di diffusione sonora ai fini evacuazione*

Un impianto di evacuazione sarà installato in tutte le aree interne ed esterne e correttamente dimensionato anche in riferimento all'alto rumore di fondo generalmente presente nelle dataroom. Tale impianto sarà interfacciato con il sistema di rilevazione fumo, ma avrà anche la possibilità di comando manuale attraverso una postazione generalmente presente nella security room.

#### 5.2.6.3 *Impianto di supervisione BEMS*

Il monitoraggio e controllo di tutta l'infrastruttura tecnologica sarà garantito dai sistemi BEMS (Building Electrical Management System). I sistemi dovranno essere attivi e funzionanti H24 sempre e comunque. L'architettura informatica hardware e software permette la fruibilità e l'utilizzo delle piattaforme anche in caso di guasto di un elemento costituente l'infrastruttura stessa.

Sulla piattaforma saranno catalogati e memorizzati tutti gli allarmi, le anomalie e le condizioni di funzionamento delle diverse apparecchiature, con la possibilità di visualizzare e storicizzare trend di temperature, umidità, assorbimenti elettrici o altre grandezze ritenute sensibili per la corretta gestione del Data Center.

Il sistema inoltre sarà in grado di trasmettere warning ed allarmi mediante email, sms o altre tecnologie ritenute adeguate allo scopo.

#### 5.2.6.4 *Impianto di estinzione incendio*

Tutte le aree critiche del Data Center saranno protette da impianti di spegnimento incendio automatico. Gli impianti saranno adeguatamente dimensionati e realizzati in riferimento alle condizioni di rischio, ai locali da proteggere ed alle logiche di attivazione.

I Dc saranno dotati di impianti di spegnimento a gas (con l'utilizzo di gas di ultima generazione conformi al protocollo di Kyoto) in luogo di impianti di spegnimento ad acqua.

#### 5.2.6.5 *Sistema di deposito gasolio*

I sistemi di stoccaggio gasolio sono opportunamente progettati in accordo con le regole tecniche di prevenzione incendi ed i decreti ministeriali ad esse associate.

Le stazioni di emergenza avranno serbatoi di stoccaggio indipendenti e possibilmente posizionati in aree diverse all'interno dell'insediamento.

Il sistema di stoccaggio potrà essere costituito da uno o più serbatoi per ogni stazione di emergenza e garantirà l'alimentazione della sorgente per un tempo non inferiore alle 48 ore in caso di alimentazione di tutto il carico elettrico del Data Center.



TIM - Uso Interno - Tutti i diritti riservati.

Il collegamento tra il sistema di stoccaggio gasolio e la stazione di emergenza sarà realizzato da tubazioni opportunamente protette dalla possibilità di congelamento del gasolio. Sarà inoltre presente un sistema di rilevamento perdite gasolio interfacciato coi i sistemi di monitoraggio dell'insediamento.

Ogni sistema di pompaggio del combustibile sarà realizzato con almeno una configurazione N+1 delle pompe elettriche + la presenza obbligatoria di una pompa ad azionamento manuale.

### 5.2.7 Impianti security

La sicurezza fisica fa parte dell'infrastruttura fisica del Data Center perché ricopre un ruolo fondamentale per ottimizzarne la disponibilità ("uptime"). In tal modo, è possibile ridurre i tempi di fermo dovuti a incidenti o sabotaggi causati dalla presenza di persone inutili o dannose.

Il Data Center avrà un piano di sicurezza semplice: la mappa dell'infrastruttura fisica identificherà le zone e i varchi di accesso che richiedono diverse regole di accesso o livelli di sicurezza.

I confini di queste zone dovranno essere preferibilmente concentrici:

- Perimetro della sede;
- Perimetro dell'edificio;
- Zona computer;
- Sale computer;
- Rack con le apparecchiature.

All'ingresso al sito sarà opportunamente predisposta una postazione di guardiania per l'esecuzione di accurati controlli a vista, ovvero analisi anche con sistemi avanzati per l'individuazione di materiale e/o sostanze pericolose all'interno di zaini, borse o altro (per le persone) e imballi (per il materiale).

#### 5.2.7.1 *Impianto controllo accessi*

L'impianto controllo accessi garantirà l'accesso a tutte le aree del Data Center con le seguenti modalità:

- Spazi non sensibili:
  - Accesso e uscita con badge + pin o sistemi equivalenti (2 livelli di controllo);
- Datarooms:
  - Accesso e uscita con antipass back ed anti accodamento con badge + pin o sistemi equivalenti (2 livelli di controllo);
- Locali tecnici:
  - Il controllo accessi alle sedi deve avvenire almeno tramite lettore di badge;



TIM - Uso Interno - Tutti i diritti riservati.

- Il controllo accessi alle aree critiche deve avvenire con letture di badge + biometrico/pin ovvero con doppio livello di controllo.

Il sistema di controllo accessi sarà gestito dalla security e registrerà tutti gli accessi ed i transiti per almeno 60 giorni.

#### 5.2.7.2 *Impianto antintrusione*

Il sito sarà equipaggiato con un sistema antintrusione ad attivazione automatica interconnesso con sistemi di vigilanza pubblica e/o privata.

L'impianto sarà caratterizzato da sensoristica di protezione perimetrale esterna all'insediamento, sensori di protezione sulle aree di accesso all'edificio, sensori di protezione sui varchi di accesso delle aree interne critiche e sensibili. Alcune aree saranno allarmate H24, altre saranno allarmate in alcune fasce orarie. Sarà possibile escludere le zone in modo selettivo al fine di garantire accessi al personale e/o a clienti e fornitori. L'esclusione della protezione potrà essere eseguita solo dal personale della security mediante opportuni codici univoci. Le esclusioni saranno tracciate e comunicate ai sistemi di vigilanza al fine di garantire almeno un doppio livello di controllo.

Il personale di vigilanza sarà presente in sito H24 con almeno 2 persone. È prevista una ronda programmata con sistema di verifica e conferma installato nelle varie aree del sito.

#### 5.2.7.3 *Impianto di videosorveglianza a circuito chiuso*

Tutto il sito sarà protetto da impianto di videosorveglianza e videoregistrazione. La registrazione delle immagini dovrà garantire uno storico non inferiore a 15 giorni per tutte le telecamere installate. L'accesso al sistema è garantito solo ed esclusivamente al personale di sicurezza adeguatamente identificato dalle procedure e normative in termini di privacy.

L'impianto dovrà garantire:

- Protezione totale perimetrica esterna dell'insediamento;
- Protezione di tutte le aree di accesso all'edificio;
- Protezione di tutte le porte di accesso ai locali tecnologici;
- Protezione di tutte le porte di accesso alle dataroom.
- Protezione di tutte le aree di ricevimento merci;
- Protezione di tutte le aree di movimentazione merci, corridoi, etc.

Nella Control Room di sicurezza saranno presenti più monitor con la visualizzazione in continuo delle aree più sensibili. Il sistema di videosorveglianza dovrà essere interfacciato con il sistema antintrusione e controllo accessi in modo che qualsiasi anomalia su questi sistemi attivi ed evidenzi l'immagine del varco e/o area laddove l'anomalia è stata rilevata.



TIM - Uso Interno - Tutti i diritti riservati.

### 5.2.8 Architetture di rete

#### 5.2.8.1 *Rete di distribuzione primaria ingresso provider*

L'infrastruttura del Data Center garantirà almeno due ingressi dall'esterno indipendenti per le connessioni dati. I due entry point dovranno, per quanto possibile, essere in punti contrapposti dell'insediamento.

Tali punti saranno entrambi interconnessi con entrambe le Meet me rooms mediante tubazioni ovvero canalizzazioni indipendenti ed opportunamente identificate utilizzate solo per questo scopo.

#### 5.2.8.2 *Rete di distribuzione secondaria*

Dai due locali Meet me room ad ogni dataroom saranno presenti canalizzazioni e/o percorsi disponibili per le interconnessioni dati. Conformemente al rating, tali percorsi saranno realizzati in compartimenti antincendio diversi ed indipendenti fino all'ingresso delle dataroom stesse.

#### 5.2.8.3 *Locali Meet me room*

I locali Meet me room rappresentano i punti di sbarco dei vari provider. Saranno presenti almeno due Meet me room per il Data Center. I due locali dovranno essere indipendenti e compartimentati tra loro. Dalle Meet me room dovrà essere possibile raggiugere qualsivoglia dataroom con l'utilizzo delle canalizzazioni di distribuzione secondaria sopra descritte.



TIM - Uso Interno - Tutti i diritti riservati.

**Proposta per la realizzazione secondo il modello del Partenariato Pubblico Privato del Polo Strategico Nazionale**

# Specificazione delle caratteristiche del servizio e della gestione

---

10 dicembre 2021

Rev. 2.0

TIM - Uso Interno - Tutti i diritti riservati.

# Sommario

1 PREMESSA ..... 4
1.1 Glossario ..... 5
2 SPECIFICHE DEL SERVIZIO ..... 6
2.1 Continuità Operativa ..... 7
2.1.1 Set up ..... 7
2.1.1.1 Obiettivi principali ..... 7
2.1.1.2 Leadership and Committment ..... 7
2.1.1.3 Ruoli Organizzativi, responsabilità ed autorità ..... 8
2.1.1.4 Risorse e Competenze ..... 8
2.1.1.5 Comunicazione ..... 9
2.1.1.6 Sub-fornitori e terze parti necessari all'erogazione dei servizi e alla loro ripartenza ..... 9
2.1.1.7 Awareness ..... 10
2.1.1.8 Documentazione ..... 10
2.1.2 Piani ed esercizi di continuità operativa ..... 11
2.1.2.1 Business Impact Analysis ..... 11
2.1.2.2 Risk Assessment ..... 12
2.1.2.3 Procedure di Business Continuity ..... 12
2.1.2.4 Business Continuity e Disaster Recovery ..... 13
2.1.2.5 Coinvolgimento di Clienti e parti interessate ..... 15
2.1.3 Performance evaluation, controlli and improvement ..... 15
2.1.3.1 Valutazione delle prestazioni ..... 15
2.1.3.2 Reporting ..... 15
2.1.3.3 Assessment e audit ..... 15
2.1.3.4 Improvement ..... 16
2.2 Console Unica ..... 16
2.2.1 Overview delle caratteristiche funzionali ..... 17
2.2.2 Modalità di accesso ..... 18
2.2.3 Interfaccia applicativa della Console Unica ..... 18
2.3 Gestione e Monitoraggio ..... 20
2.3.1 Gestione SW Infrastrutturale ..... 21
2.3.2 Gestione SW Operativo ..... 21
2.3.3 Gestione HW ..... 21
2.3.4 Modalità di esecuzione dei servizi e delle attività ..... 21
2.3.5 Collaudi e verifiche di conformità ..... 23

2.4 Security Management ..... 24
2.4.1 Modello di servizio DDOS ..... 24
2.5 Servizio di Assistenza e Manutenzione ..... 25
2.5.1 Centro di Gestione ..... 26
2.5.2 Servizio di Contact Center ..... 26
2.5.2.1 Trouble Ticketing System ..... 27
2.6 Service Management ..... 28
2.7 SLA Management ..... 28
2.7.1 Calendario degli interventi ..... 28
2.8 Assicurazione della Qualità ..... 29
2.8.1 Audit Qualità ..... 30
2.8.2 Audit Sicurezza ..... 30
3 Chiusura della Fornitura ..... 30
4 Portale di Fornitura ..... 31

## Indice delle Figure

Figura 1 – Schema funzionale della Console Unica ..... 16
Figura 2 – Funzionalità CU ..... 17
Figura 3 – Dashboard CU ..... 19
Figura 4 - Esempio organizzazione Contact Center ..... 27
Figura 5 - Esempio di Mappa di navigazione del Portale ..... 31

# Lista delle revisioni

| Rev. | Data | Descrizione |
|---|---|---|
| 1.0 | 27/09/2021 | Prima versione del documento |
| 2.0 | 10/12/2021 | Seconda versione del documento.<br>Correzioni refusi e controllo ortografico.<br>Modificati paragrafi:<br>2.5 Servizio di Assistenza e Manutenzione<br>2.7.1 Calendario degli interventi |

# 1 PREMESSA

Il presente documento ha l'obiettivo di illustrare le modalità di esecuzione della Fornitura descritta nel documento "Progetto fattibilità" che ha come oggetto l'erogazione dei seguenti servizi:

- Servizi **Infrastrutturali on-demand:**
  - **Industry Standard (Hosting, Housing, IaaS, PaaS, BaaS);**
  - **Public Cloud PSN Managed;**
  - **Secure Public Cloud;**
  - **Public PaaS on PSN Site;**
- Servizi di **Migrazione, Evoluzione e Professional Services;**
- Servizi di **Gestione della Sicurezza IT, a standard ISO 27001;**
- Servizi di **Disaster recovery** e **Business Continuity, a standard ISO 22301;**
- Servizi di **Assistenza** ai fruitori dei servizi erogati;
- **Console Unica** di gestione.

Tutti i termini temporali (giorni, mesi, anni) indicati nel presente documento devono intendersi come "solari", ove non diversamente previsto.

## 1.1 Glossario

Salva diversa esplicita indicazione, ai termini seguenti, riportati in ordine alfabetico, viene attribuito, ai fini del presente documento, il significato di seguito indicato.

| TERMINE | DEFINIZIONE |
|---|---|
| Applicazione | Una qualsiasi realizzazione software (ad-hoc o prodotto di mercato) tesa a fornire un insieme di funzionalità alla PA. Solitamente una applicazione è composta da uno o più moduli software e da un database a cui l'applicazione fa riferimento. |
| NewCo PSN | Società di scopo, |
| Contratto | L'atto che verrà stipulato tra la PA ed il NewCo PSN, nel quale sono enunciate le regole giuridiche alle quali si dovrà conformare il Servizio. |
| Centro Servizi | Il Centro Servizi del NewCo PSN rappresenta l'insieme di tutte le infrastrutture fisiche (Data Center), delle componenti hardware e software in essi ospitati e delle risorse destinate all'erogazione dei Servizi oggetto del presente Progetto di fattibilità. |
| Fornitura | L'insieme dei prodotti software, hardware, dei servizi e di tutto ciò che è richiesto nel presente Progetto di Fattibilità. |

| TERMINE | DEFINIZIONE |
|---|---|
| Servizi professionali | Gestione applicativa, supporto specialistico, servizio di assistenza da remoto, se richiesto, |
| SLA | Service Level Agreement, ovvero “indicatori di prestazione chiave”, e cioè quegli indicatori che permettono di misurare le prestazioni di una determinata attività o di un determinato processo. |

# 2 SPECIFICHE DEL SERVIZIO

I Servizi oggetto della Fornitura descritta nel documento “*Progetto di Fattibilità*” saranno erogati in modalità continuativa, fatto salvo il verificarsi di esigenze estemporanee del Committente che determinino la necessità di sospendere la Fornitura. La modalità continuativa presuppone che l'erogazione del servizio sia senza soluzione di continuità per tutta la durata del contratto, a decorrere dall’attivazione dello stesso. Tale modalità comprende sia le attività pianificabili già all’inizio della fornitura, sia tutte le altre che lo saranno solo in funzione delle esigenze che si manifesteranno di volta in volta.

All’interno del presente Servizio è ricompresa ogni prestazione e attività atta a garantire la continuità, la piena funzionalità e l’efficienza degli impianti tecnologici infrastrutturali del Data Center al fine di mantenere inalterate nel tempo le prestazioni, le caratteristiche e la funzionalità dell’infrastruttura IT e TLC delle PAC.

In caso di guasto, la NewCo PSN si impegna a ripristinare la perfetta funzionalità e la piena disponibilità degli impianti e delle macchine attraverso interventi di riparazione, garantendo la disponibilità del servizio e i tempi di ripristino secondo quanto previsto dagli indicatori di qualità proposti all’interno del presente Progetto di Fattibilità.

Si intendono, altresì, inclusi nell’oggetto del Servizio, i servizi di gestione delle interconnessioni e connettività, dell’infrastruttura hardware e software IT, degli impianti tecnologici infrastrutturali dei Data Center, nonché i servizi di conduzione e manutenzione dei suddetti impianti e delle componenti edili ad essi relativi presenti presso i siti della NewCo PSN.

La NewCo PSN, nell’espletamento dei servizi oggetto di Fornitura, assicurerà la qualità dei servizi richiesta proponendo un Modello generale dove regolamentare le interazioni con le PA, in particolar modo a supporto degli stessi in caso di malfunzionamenti o indisponibilità del Servizio.

La NewCo PSN si farà inoltre carico di tutte le attività di progettazione e set up della Gestione Operativa, propedeutico all’erogazione dei Servizi descritti nel documento “*Progetto di Fattibilità*”.

La Control Room sarà situata in uno stabile diverso dai quattro Data Center previsti.

## 2.1 Continuità Operativa

La NewCo PSN apporterà le appropriate misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi richiesti, a fronte di gravi emergenze che ne intacchino la regolare attività, in coerenza con le evoluzioni della tecnologia e che preveda test ripetuti per garantire l'adeguatezza e l'aggiornamento continuo delle soluzioni tecniche e organizzative adottate.

La NewCo PSN si impegna a descrivere il proprio sistema di **Gestione della Continuità Operativa – Business Continuity Management System**, in linea con i requisiti dello standard ISO 22301:2012 e dello standard ISO 27001.

Dovrà quindi mettere a disposizione 4 Data Center attrezzati e dedicati al PSN, certificati Tier IV di cui 2 anche con disponibilità di sale Tier III, localizzati in doppia Region che abbiano tutte le caratteristiche di sicurezza e capacità elaborativa per erogare i servizi richiesti dal presente documento di specificazione del servizio e della gestione.
Tutti i servizi elencati nel presente capitolo sono previsti come necessari nelle modalità di erogazione dei servizi infrastrutturali previsti (Housing, Hosting e Iaas).

### 2.1.1 Set up

La NewCo PSN metterà in atto un processo continuo di gestione e di governo che garantirà di intraprendere i passi necessari al fine di identificare l'impatto di potenziali perdite, di mantenere praticabili i piani e le strategie di ripristino e di assicurare la continuità dei prodotti e dei servizi mediante programmi di formazione, test, esercitazioni e costanti attività di aggiornamento e revisione.

A titolo esemplificativo e non esaustivo, indichiamo le componenti che dovranno essere previste dalla NewCo PSN per il proprio Business Continuity Management System.

#### 2.1.1.1 **Obiettivi principali**

L'obiettivo principale del Business Continuity Management System sarà quello di garantire che la NewCo PSN sia in grado di reagire a fronte di eventi dannosi che ne minacciano la sopravvivenza o l'immagine nel rispetto delle normative di riferimento e di quanto definito nei contratti con le PA.

I principi che stabiliscono le priorità nella gestione dell'emergenza/crisi e che orientano le decisioni saranno:

- proteggere la vita e l'incolumità delle persone;
- prevenire ulteriori conseguenze derivanti dall'incidente di origine;
- proteggere la continuità del business e tutelare il patrimonio di immagine dell'azienda;
- cooperare alla garanzia di continuità di erogazione del sistema Pubblico;
- salvaguardare i beni di cui l'azienda ha la disponibilità o la responsabilità, nel rispetto dell'ambiente.

#### 2.1.1.2 **Leadership and Committment**

Per quanto concerne il Sistema di Governo della Business Continuity (BCMS) la NewCo PSN:

- Identificherà i principali ruoli di Business Continuity all'interno delle singole unità aziendali, ossia costituirà una struttura organizzativa competente che si occuperà della gestione e dell'implementazione della Business Continuity in azienda ed una struttura organizzativa predefinita per la gestione straordinaria delle emergenze e delle crisi.
- Definirà e diffonderà la Politica per la Business Continuity, dalla quale discendono le Strategie d'azione, le Linee Guida e gli obiettivi della Business Continuity.
- Favorirà la comprensione dell'azienda attraverso l'identificazione dei suoi servizi chiave e delle sue attività critiche, nonché delle risorse necessarie per il loro mantenimento, attraverso lo svolgimento delle attività di Business Impact Analysis e Risk Assessment.

La NewCo PSN, inoltre, garantirà nel perimetro dei Servizi in fornitura:

- Lo sviluppo e l'aggiornamento di piani, istruzioni e processi che la mettano in grado di gestire prontamente le emergenze e le crisi.
- La definizione di una struttura documentale contenente l'insieme dei piani predefiniti che dettagliano come l'organizzazione gestisce un evento dannoso e come garantisce la continuità delle sue attività in caso di disastro.
- La predisposizione di programmi periodici di formazione sulla Business Continuity.
- La pianificazione di test ed esercitazioni periodiche di Business Continuity e di Disaster Recovery.
- La revisione periodica di tutto il Business Continuity Management System per assicurare la sua rispondenza ed adeguatezza a fronte di cambiamenti normativi, organizzativi, strategici e legislativi.

#### 2.1.1.3 **Ruoli Organizzativi, responsabilità ed autorità**

La NewCo PSN identificherà ruoli e responsabilità al proprio interno per fronteggiare aspetti organizzativi (Business Continuity), tecnologici (Disaster Recovery) e logistici, istituendo modalità organizzative e operative per:

- coordinare lo sviluppo delle tematiche inerenti la Business Continuity e la resilienza nell'erogazione dei servizi e nei progetti applicativi ed infrastrutturali;
- ~~e~~ sviluppare integrare tali azioni in un programma di Risk Management e presidiare e monitorare l'individuazione e l'analisi dei rischi e dei piani di trattamento dei rischi individuati.

#### 2.1.1.4 **Risorse e Competenze**

La NewCo PSN si impegna a perseguire gli obiettivi di Business Continuity con le risorse e i mezzi adeguati e a conferire ai ruoli di Business Continuity l'autorità e le risorse necessarie per svolgere i loro compiti.

Si impegna inoltre ad individuare le risorse necessarie all'attuazione del Sistema di Governo della Business Continuity in sintonia con la politica e gli obiettivi di Business Continuity per il conseguimento della soddisfazione del Cliente.

Tali risorse si identificheranno nel personale competente ed adeguatamente addestrato, nelle informazioni e sistemi informativi di supporto, nelle infrastrutture, negli ambienti di lavoro e nelle tecnologie utilizzate.

La NewCo PSN si impegna a mettere a disposizione ogni anno, nel budget aziendale, le risorse necessarie per la gestione e l'evoluzione della Business Continuity.

#### 2.1.1.5 Comunicazione

Durante uno stato di crisi sarà molto importante gestire il processo di comunicazione sia verso l'interno che verso l'esterno.

La responsabilità del processo di comunicazione verso i clienti durante uno stato di crisi sarà assegnata ad una apposita funzione che garantirà il presidio della strategia di comunicazione da adottare nei confronti dei media, intervenendo operativamente presso gli stessi in maniera proattiva o in risposta a specifiche richieste e predisponendo i messaggi standard da divulgare agli stakeholder esterni.

#### 2.1.1.6 Sub-fornitori e terze parti necessari all'erogazione dei servizi e alla loro ripartenza

La NewCo PSN identificherà i suoi sub-fornitori, partner, terze parte di ritenere essenziali per l'erogazione dei servizi e per la loro ripartenza. Tale elenco sarà costantemente aggiornato e fornito su richiesta al cliente.

La NewCo PSN garantirà che i livelli di servizio e le obbligazioni contrattuali che lo impegnano verso i Clienti siano riproposte nelle obbligazioni contrattuali verso subfornitori e terze parti essenziali.

La NewCo PSN assicurerà il pieno accesso e la massima trasparenza dei suoi sub-fornitori e terze parti nel caso di verifiche di audit da parte dei Clienti e nel caso di verifiche e controlli avviati dalla Autorità di Vigilanza sui Clienti.

La NewCo PSN valuterà il potenziale impatto che una interruzione o una mancata prestazione del servizio potrebbe avere sui livelli di servizio contrattualizzati su base continuativa ricomprendendo tale esercizio in un proprio piano di continuità operativa.

La NewCo PSN assicura che i propri sub-fornitori siano in possesso della certificazione ISO/IEC 27001 per i processi relativi alle attività in perimetro di fornitura nonché si conformino alle policy di sicurezza definite dal **Soggetto** costituito.

La NewCo PSN ha l'obbligo di proteggere le informazioni riservate, personali o altrimenti sensibili e di rispettare tutti gli obblighi normativi relativi alla protezione dei dati personali. A tale fine effettuerà test periodici di penetrazione per valutare l'efficacia delle misure e dei processi di sicurezza ICT interni e a difesa da attacchi esterni.

Più in generale la NewCo PSN prevede una documentata analisi preventiva dell'esternalizzazione, volta a valutare tutti i rischi dell'accordo e ad effettuare una adeguata due diligence sulla potenziale NewCo PSN.

Tutte le informazioni concernenti gli accordi di esternalizzazione saranno documentati e conservati dalla NewCo PSN anche dopo la cessazione per un periodo di tempo adeguato. Estremi e contenuti degli accordi verranno conservati in modo idoneo.

La NewCo PSN si assicurerà di poter porre termine agli accordi di esternalizzazione senza interrompere indebitamente le proprie attività operative, senza limitare il rispetto degli obblighi normativi e senza pregiudicare la continuità e la qualità dei servizi forniti ai propri clienti.

#### 2.1.1.7 **Awareness**

La NewCo PSN avrà un piano per formare il personale e mettere in condizioni di fronteggiare gli scenari di crisi e le problematiche organizzative (Business Continuity), tecnologiche (Disaster Recovery) e logistiche. Tale programma sarà appositamente documentato e coinvolgerà tutto il personale preposto alla ripartenza dei servizi.

Tale piano potrà essere portato all'attenzione dei clienti qualora venga richiesto

#### 2.1.1.8 **Documentazione**

Tutta la documentazione emessa per il Sistema di Gestione della Business Continuity (BCMS) sarà archiviata in elettronico su un sistema documentale della NewCo PSN in alcune librerie nelle quali sono archiviate sia la documentazione aziendale, sia la documentazione di direzione, sia la documentazione operativa per il ripristino dei servizi.

La NewCo PSN assicurerà la disponibilità della documentazione, in formato elettronico o cartaceo, a tutto il personale e presso tutte le sedi coinvolti nella gestione degli scenari di crisi.

La NewCo PSN assicurerà, inoltre, il mantenimento del sistema tramite un processo di aggiornamento della documentazione grazie al quale ogni cambiamento, interno ed esterno, che abbia impatto sulla Fornitura, viene recepito all'interno della gestione della Business Continuity/Disaster Recovery.

Inoltre, la NewCo PSN si impegna ad effettuare periodicamente, o a fronte di variazioni rilevanti, una revisione di tutto il Sistema di Gestione della Business Continuity (BCMS) per assicurare la sua rispondenza ed adeguatezza a fronte di cambiamenti normativi, organizzativi, strategici e legislativi.

Tra la documentazione da predisporre, prevedere e mantenere aggiornata si riporta ad esempio:

- Business Continuity and Disaster Recovery strategies.
- Business Continuity and Disaster Recovery solutions.
- RTO calculation methodology.
- Business Continuity and Disaster Recovery test methodology.
- Business Continuity and Disaster Recovery tests minutes.
- Business Continuity and Disaster Recovery corrective actions.
- BCDR Plan awareness.

### 2.1.2 Piani ed esercizi di continuità operativa

Obiettivo del Servizio di Business Continuity è garantire che la struttura aziendale sviluppi piani, istruzioni e processi e renda disponibili locali ed apparecchiature in modo tale da essere in grado di gestire prontamente gli incidenti e le crisi.

Lo sviluppo e l'attuazione di una risposta di Business Continuity derivano dalla creazione di un modello di gestione e da una struttura di gestione dell'evento disastroso, di piani di Business Continuity e Disaster Recovery che dettagliano i passi da compiere durante e dopo un incidente per conservare o ripristinare l'operatività.

Il Sistema dovrà permettere di:

- confermare la natura e l'estensione dell'incidente;
- dare l'avvio ad un'appropriata risposta di Business Continuity;
- avere piani, processi e procedure per l'attivazione, il coordinamento, la comunicazione, la gestione e la chiusura dell'emergenza;
- avere a disposizione le risorse per supportare i piani, i processi e le procedure nella gestione dell'incidente;
- comunicare con gli stakeholder, ovvero i principali attori coinvolti.

La NewCo PSN svolgerà la propria attività in ambienti complessi ed altamente competitivi, erogando servizi che possono avere un impatto sull'intero sistema Pubblico Nazionale. Per questo motivo assume una rilevanza fondamentale il pieno rispetto dei requisiti di continuità operativa derivanti dalle normative di riferimento, dai requisiti dettati dalle Autorità di Vigilanza e dai contratti commerciali con i Clienti.

Per raggiungere questo obiettivo la NewCo PSN opererà in coerenza con le metodologie, le best practice e gli standard internazionali di riferimento, producendo e mantenendo aggiornati la Business Impact Analysis e il Risk Assessment, definendo la strategia di Business Continuity, le procedure di tipo organizzativo, logistico e tecnologico ed effettuando regolarmente esercitazioni e test come di seguito illustrato.

#### 2.1.2.1 Business Impact Analysis

La Business Impact Analysis (BIA) è la valutazione dell'impatto sul business in caso di eventi di rilievo che possono compromettere le attività aziendali e l'erogazione dei servizi. Al fine di indirizzare appropriate soluzioni di Business Continuity, vengono identificati i requisiti di ripartenza dei servizi.

La NewCo PSN produrrà la Business Impact Analysis con l'obiettivo di:

- Censire i servizi rilevanti per il business aziendale.
- Identificare gli impatti legati all'indisponibilità del servizio.
- Identificare i tempi di ripristino a livello contrattuale/normativo.
- Identificare i servizi maggiormente critici.
- Identificare quali attività hanno la necessità di essere ripristinate in un momento successivo.

La Business Impact Analysis riporterà principalmente l'analisi dei servizi di business e l'individuazione delle attività critiche utilizzando i parametri di valutazione che tengono conto di vincoli a livello normativo, vincoli contrattuali con i clienti, rilevanza del servizio/attività per il business aziendale, rilevanza strategica del servizio/attività per l'azienda.

La BIA sarà aggiornata con le informazioni fornite dalle strutture aziendali coinvolte e resa disponibile all'azienda per la predisposizione dei piani di Disaster Recovery.

#### 2.1.2.2 **Risk Assessment**

Il Risk Assessment sarà finalizzato alla prevenzione e al contrasto delle minacce che possono colpire gli asset aziendali provocandone, tra gli altri impatti, l'indisponibilità per un periodo più o meno prolungato.

Con l'effettuazione del Risk Assessment, la NewCo PSN si propone di proteggere il valore aziendale, perseguire gli obiettivi aziendali e gestire i rischi che potrebbero comportare la perdita di riservatezza, integrità, disponibilità e conformità dei servizi/processi aziendali.

Il processo di gestione dei rischi della NewCo PSN sarà riferito in prima istanza allo standard ISO 31000. In esso sarà descritto come i rischi sono identificati, analizzati, valutati, trattati, monitorati e aggiornati con le relative responsabilità.

La decisione sul trattamento dei rischi individuati, basata sulla valutazione del giusto equilibrio fra rispetto delle norme cogenti, necessità di business, di costo, tecnologiche e di sicurezza, sarà declinata nelle classiche opzioni di trattamento dei rischi (mitigare, accettare, evitare, trasferire).

Sulla base delle decisioni assunte, varrà compilato il cosiddetto Piano di Trattamento dei Rischi, che conterrà le modalità che la NewCo PSN avrà deciso di adottare per trattare i rischi individuati.

La NewCo PSN obbligatoriamente aggiornerà periodicamente e monitorerà in modo sistematico il proprio Piano di Trattamento dei Rischi.

Periodicamente la NewCo PSN obbligatoriamente produrrà il documento Rischi di Sicurezza Fisica (Security) per ciascuna delle sedi aziendali ed eseguirà l'analisi dei rischi a livello Safety coerentemente con la legge 81/08.

#### 2.1.2.3 **Procedure di Business Continuity**

La NewCo PSN predisporrà un Processo di Gestione delle Emergenze e dello Stato di Crisi al fine di descrivere le modalità di attivazione, le responsabilità ed i contatti necessari per gestire una situazione di emergenza o e/o crisi in azienda.

Il Processo di Gestione delle Emergenze e dello Stato di Crisi è caratterizzato da tre fasi: Incidente, Emergenza e Crisi.

La NewCo PSN distinguerà gli eventi sulla base degli impatti che possono avere (ICT, NO ICT, Cyber), individuando in questo modo sia le procedure di gestione degli incidenti da seguire, sia i Team da coinvolgere.

L'attivazione del Processo di Gestione delle Emergenze e dello Stato di Crisi si renderà necessaria quando l'evento presenta rischi e impatti di gravità tale da non poter essere gestito mediante le procedure di gestione degli incidenti in essere presso la NewCo PSN.

Le azioni da porre in essere e le relative responsabilità di esecuzione nel caso in cui si presenti uno stato di emergenza o che impone l'evacuazione dello stabile o di alcune zone per preservare l'incolumità delle persone dovranno essere descritte in specifici documenti.

A completamento del Processo di Gestione delle Emergenze e dello Stato di Crisi, sarà necessario che la NewCo PSN condivida il Business Continuity Plan (BCP) ed il Disaster Recovery Plan della Fornitura, andando a descrivere le modalità organizzative da seguire per il ripristino e il controllo dei propri servizi.

#### 2.1.2.4 **Business Continuity e Disaster Recovery**

Nello specifico, nel **Business Continuity** Plan sarà necessario descrivere:

- gli scenari di disastro ipotizzati;
- la gestione dei contatti e delle comunicazioni durante l'emergenza o crisi (risorse interne, fornitori, clienti, società partecipate/controllate);
- le azioni di contenimento e/o di contrasto ipotizzate per ogni scenario;
- la documentazione di riferimento per ogni servizio;
- i nominativi di riferimento del personale operativo da coinvolgere– ivi compreso i sub-fornitori se presenti.

La NewCo PSN assicura il costante aggiornamento del piano in modo che sia rispondente alla evoluzione dei servizi, delle tecnologie e delle infrastrutture necessarie ad erogare il servizio stesso.

Il **Disaster Recovery** Plan è un insieme di documenti redatti per il ripristino delle infrastrutture tecniche e applicative che descrivono le modalità e la tempistica di riattivazione presso il sito di Disaster Recovery.

L'erogazione dei servizi in Disaster Recovery sarà garantita da soluzioni hardware, software e di connettività dedicate e dalla disponibilità di personale interno con adeguata preparazione.

Le soluzioni tecnologiche garantiranno l'interconnessione fra i siti e gli accessi logici remoti ai siti stessi. Il sito di DR sarà allestito con piattaforme tecnologiche dotate di capacità elaborativa equivalente a quelle del sito primario. I dispositivi hardware saranno ridondati o avranno adeguate caratteristiche di fault tolerant per assicurare i requisiti di DR dei servizi.

Il principale scenario di disastro che dovrà essere gestito è quello di Disaster Recovery di sito infrastrutturale.

Le soluzioni architetturali di BC (intra Region) adottate sono dimensionate per poter garantire una configurazione di tipo High Availability (HA) tra DC della stessa Region. Inoltre, le soluzioni adottate permetteranno di realizzare specifiche tipologie di configurazione dell'infrastruttura tecnologica, garantendo, in base alle caratteristiche del servizio, la soddisfazione con valori di RTO Recovery Time Objective e di RPO Recovery Point Objective maggiori o uguali di quelli riportati nella seguente tabella:

| RTO | RPO |
|---|---|
| 30 minuti | 1 minuto |

Nel caso le PAC richiedessero, tramite specifici progetti, la gestione di scenari differenti ad esempio DR su diversa Region, la NewCo PSN sarà in grado di garantire valori di RTO e RPO almeno pari a:

| Scenario | RTO* | RPO |
|---|---|---|
| DR sito infrastrutturale | 4 ore | 30 minuti |

*RTO calcolato dal momento della decisione di attivare il Disater Recovery

La soluzione di DR resa disponibile prevede la possibilità di abilitare la configurazione di metriche di replica full mesh tra i DC costituenti le differenti Region al fine di garantire alla PAC la possibilità di scegliere la più idonea configurazione alle proprie esigenze di collocazione dei workload attivi e delle relative istanze di replica.

Un Business Continuity Management System non può considerarsi affidabile se non viene regolarmente testato ed aggiornato adeguatamente, quindi la NewCo PSN effettuerà periodicamente test ed esercitazioni di Business Continuity e di Disaster Recovery, che potranno essere di tipo:

- **organizzativo** (ad esempio: Test del Processo di Gestione delle Emergenze, test dei Business Continuity Plan, etc.);
- **logistico** (prove di evacuazione degli edifici);
- **tecnologico** (test di Disaster Recovery).

La NewCo PSN prevede di effettuare questi test annualmente, definendo per tempo le modalità di partecipazione ai test di Clienti e altri parti interessate. Alla conclusione del test sarà predisposto un apposito documento di reporting contenente l'esito del test, i punti di miglioramento rilevati e i conseguenti dei piani di rientro predisposti.

I test di Business Continuity saranno effettuati per verificare l'efficacia e l'efficienza del Processo di Gestione delle Emergenze, per verificare l'adeguatezza, la completezza e la funzionalità dei Business Continuity Plan e delle procedure a supporto, per valutare la preparazione dei gruppi di gestione della Business Continuity e l'efficacia del programma di awareness, per sviluppare e diffondere la conoscenza e la sensibilità sulle tematiche di Business Continuity in azienda.

I test di Disaster Recovery saranno necessari per valutare la funzionalità e l'efficienza delle infrastrutture tecnologiche e mantenere aggiornati gli skill delle persone coinvolte.

Il test del Processo di Gestione delle Emergenze e dello Stato di Crisi (chiamato anche Call Tree test) verrà effettuato ogni anno, inoltre con cadenza annuale la NewCo PSN predisporrà il piano pluriennale dei Test di Business Continuity e dei Test di Disaster Recovery.

#### 2.1.2.5 Coinvolgimento di Clienti e parti interessate

La completa realizzazione della Business Continuity non potrà prescindere dallo sviluppo di un rapporto di collaborazione diretto con la propria clientela, che renderà possibile l'analisi, la definizione e l'implementazione di tutte le misure congiunte per la gestione della crisi e per il recupero dei servizi e delle tecnologie di supporto.

In tal senso la NewCo PSN concorderà coi propri clienti le modalità di reciproca collaborazione, quali:

- le connessioni da utilizzare in caso di disastro;
- i riferimenti da contattare per le comunicazioni generali;
- le azioni da compiere in caso di attivazione dell'infrastruttura tecnico-applicativa dal sito di Disaster Recovery;
- la pianificazione dei test.

La NewCo PSN porterà all'attenzione e all'approvazione del Cliente i Business Continuity Plan con cadenza annuale e le loro modifiche e aggiornamenti.

### 2.1.3 Performance evaluation, controlli and improvement

#### 2.1.3.1 Valutazione delle prestazioni

La NewCo PSN misurerà le performance delle seguenti attività di Business Continuity e condividerà i risultati con le PA clienti:

- Test di BC e di DR;
- Awareness;
- Verifiche ispettive interne;
- Gestione della documentazione.

I rispetti indicatori di performance saranno indicativamente:

- dei test di BC e DR, è il Severity Code assegnato ai test eseguiti;
- dell'attività di awareness, è il grado di copertura dei componenti dei team di gestione della BC;
- dell'attività delle Verifiche Ispettive Interne, è il grado di copertura delle Direzioni e Divisioni;
- della gestione della documentazione, è il numero di documenti aggiornati sul totale dei documenti del BCMS.

#### 2.1.3.2 Reporting

La NewCo PSN assicurerà una informativa su:

- Piano dei test previsti per l'anno, test condotti e loro esito.
- Piano della formazione e awareness e loro esito.
- Piano delle verifiche interne e di terza parte, azioni correttive e di miglioramento e loro esito.

#### 2.1.3.3 Assessment e audit

Al fine di perseguire il miglioramento continuo del BCMS, la NewCo PSN effettuerà periodicamente una revisione del proprio sistema al fine di verificare l'efficacia, l'efficienza e la continua adeguatezza dello stesso e delle relative politiche, strategie ed obiettivi e di identificare le eventuali necessità di adeguamento, attuando le opportune azioni correttive e di miglioramento.

Con cadenza annuale, la NewCo PSN predisporrà il Piano annuale delle Verifiche Ispettive di Business Continuity ed effettuerà le Verifiche Ispettive Interne.

I risultati delle Verifiche Ispettive di Business Continuity saranno documentati e riesaminati con i responsabili delle unità aziendali sottoposte a verifica allo scopo di concordare un piano di azioni correttive e di trattamento delle eventuali non conformità riscontrate.

Gli esiti di questo programma di verifiche e la documentazione saliente saranno messe a disposizione del Cliente con le modalità ritenute opportune per proteggere la confidenzialità delle informazioni.

#### 2.1.3.4 **Improvement**

Nel corso dello svolgimento di attività legate principalmente all'ambito della BIA, dei Test, delle Verifiche Ispettive e degli Audit (sia esterni sia interni) potranno scaturire non conformità e quindi la necessità di individuare opportune azioni migliorative o correttive.

Una azione migliorativa o correttiva è una azione definita per eliminare la causa di una non conformità e prevenirne il riaccadimento.

La NewCo PSN si impegna a migliorare con continuità il proprio BCMS utilizzando come guida le politiche per la Business Continuity, gli obiettivi di Business Continuity, i risultati delle verifiche ispettive di Business Continuity, l'analisi dei dati, le azioni correttive ed i Riesami della Direzione.

## 2.2 Console Unica

La Fornitura prevede l'erogazione alle PAC, in maniera continuativa e sistematica, di una serie di servizi afferenti ad un Catalogo predefinito e gestito attraverso una Console Unica dedicata.
La NewCo PSN metterà a disposizione delle Amministrazioni Contraenti una piattaforma di gestione degli ambienti cloud unica (CU) personalizzata, interoperabile attraverso API programmabili che rappresenterà per la PA l'interfaccia unica di accesso a tutte le risorse acquistate nell'ambito della convenzione. In particolare, la CU garantirà la possibilità alle Amministrazioni di configurare ed istanziare, in autonomia e con tempestività, le risorse contrattualizzate per ciascuna categoria di servizio e, accedendo alle specifiche funzionalità della console potrà gestire, monitorare ed utilizzare i servizi acquisiti.
Infine, attraverso la CU, l'Amministrazione avrà la possibilità di segnalare anomalie sui servizi contrattualizzati tramite l'apertura guidata di un ticket per la cui risoluzione la NewCo PSN si avvarrà del supporto di secondo livello di specialisti di prodotto/tecnologia.
Lo schema funzionale della soluzione proposta è illustrato a blocchi nella Figura 1 la cui descrizione dettagliata è riportata nei successivi paragrafi.

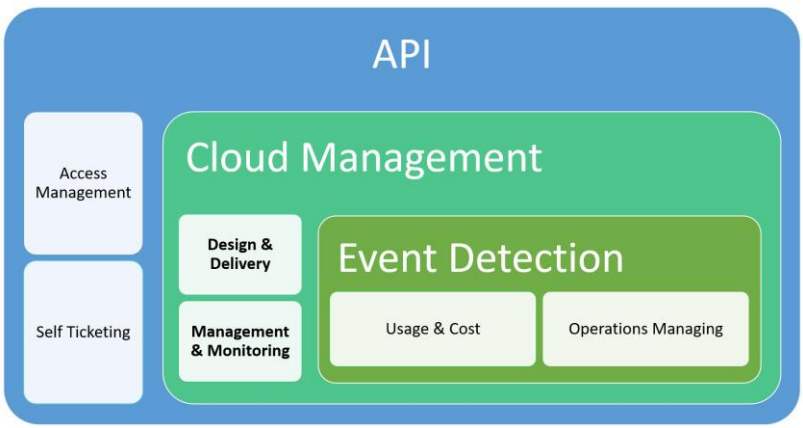



Figura 1 – Schema funzionale della Console Unica

### 2.2.1 Overview delle caratteristiche funzionali

La CU è progettata per interagire col PSN CLOUD ed integrare le funzionalità delle console native di cloud management degli OTT, fornendo un'interfaccia unica in grado di guidare in modo semplice l'utente nella definizione e gestione dei servizi sottoscritti utilizzando anche la tassonomia e le modalità di erogazione dei servizi previsti nella convenzione. Tale piattaforma presenta un'interfaccia applicativa responsive e multidevice ed è utilizzabile, oltre che in modalità desktop, anche mediante dispositivi mobili Android o iOS e abilita i sottoscrittori ad accedere in maniera semplificata agli strumenti che consentono di: √gestire in modalità integrata i profili di accesso alla CU tramite le funzionalità di Identity Management; √disegnare l'architettura dei servizi acquistati e gestirne le eventuali variazioni; √consentire l'interfacciamento attraverso le API per la gestione delle risorse istanziate ma anche per definire un modello di IaC (Infrastructure as Code); √segnalare eventuali anomalie in modalità "self".

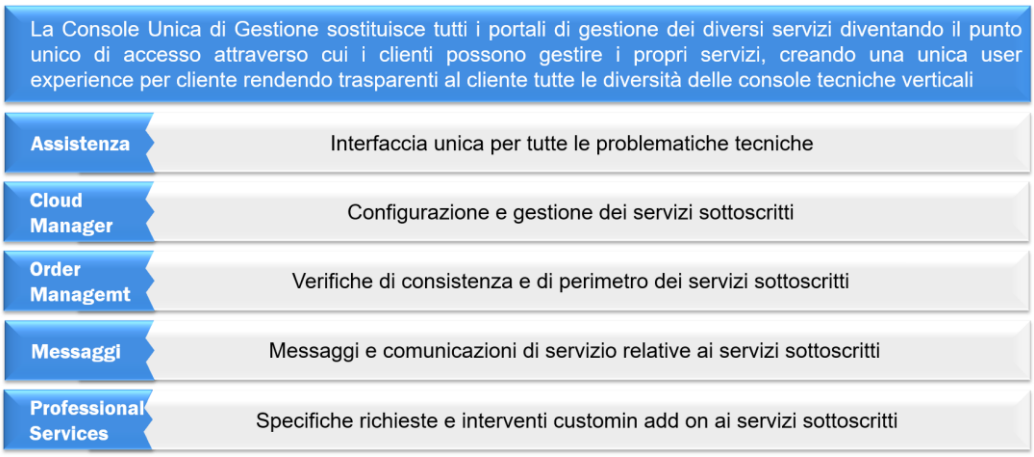



Figura 2 – Funzionalità CU

Le aree di interazione che la piattaforma CU consente di gestire sono:

1. **Area Attivazione contrattuale**

All'atto dell'adesione alla convenzione da parte dell'Amministrazione, sulla CU: √saranno caricati i dati contrattuali ed anagrafici dell'Amministrazione; √generato il profilo del referente Master (Admin) della PA a cui sarà inviata una "Welcome Letter" con il link della piattaforma, l'utenza e la password (da modificare al primo login) per l'accesso alla CU; √sarà configurato il tenant dedicato alla PA, che rappresenta l'ambiente cloud tramite il quale la PA usufruirà dei servizi acquisiti (IaaS, PaaS, ecc.).

2. **Area Access Management e profilazione utenze**

L'accesso alla CU è gestito totalmente dal sistema di Identity Access Management (IAM). Gli utenti, previa registrazione, saranno censiti nello IAM, e con le credenziali rilasciate potranno accedere dalla console alle risorse allocate all'interno del proprio tenant.
Anche la creazione dei profili delle utenze e la loro associazione con gli account degli utenti sarà gestita tramite le funzionalità di IAM in un'apposita sezione della CU denominata "Gestione Utenze".

3. **Area Design & Delivery**

Attraverso tale modulo della CU, l'Amministrazione Contraente potrà configurare in autonomia i servizi acquistati secondo le metriche definite per la convenzione, costruendo, anche mediante l'utilizzo di un tool di visualizzazione, la propria architettura cloud sulla base delle risorse contrattualizzate. Successivamente la CU, interagendo in tempo reale attraverso le API dei servizi cloud verticali, consentirà l'immediata attivazione delle risorse e dei servizi previsti nell'architettura attraverso la

creazione di uno o più tenant logici per segregare le risorse computazionali dei clienti (Project). Il processo è gestito mediante un workflow automatizzato di delivery implementato tramite l'uso di Blueprint. La CU esporrà anche delle API affinché la singola Amministrazione Contraente possa interagire attraverso i propri tools di CD/CI, IaC (Terraform, Ansible…) oppure attraverso una propria CU come ulteriore livello di astrazione e indipendenza (qualora ne avesse già a disposizione e quindi creare una CU Master Controller che interagisce con quella del PSN appunto via API).

4. **Area Management & Monitoring**

La piattaforma consentirà ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali.
Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.

5. **Area Self Ticketing**

Consente alla PA di segnalare in modalità self le anomalie riscontrate sui servizi cloud contrattualizzati.

### 2.2.2 Modalità di accesso

L'accesso in modalità sicura alla Console Unica prevede l'utilizzo del sistema di Identity Management, il cui form di login è integrato nell'interfaccia web. Tale sistema gestisce le identità degli utenti registrati e consente sia l'accesso in modalità desktop, sia tramite dispositivi mobili Android o iOS. Gli utenti, autorizzati dal sistema di Identity Access Management, potranno accedere dalla console alle risorse allocate all'interno del proprio tenant, sia per attività di "Design & Delivery" sia per attività di "Management & Monitoring".

### 2.2.3 Interfaccia applicativa della Console Unica

La Console Unica espone un'interfaccia profilata per ciascuna Amministrazione Contraente, presentando il set di servizi contrattualizzati e abilitandola ad eseguire le operazioni desiderate in piena autonomia. Di seguito è riportata una breve descrizione delle sezioni della Console Unica che sono rese disponibili. Dall'Home Page è possibile accedere alle sezioni:

• **Dashboard**: consente di visualizzare il riepilogo dei dati contrattuali, verificare lo stato dei propri servizi IaaS, PaaS, ecc, il tracking dei ticket aperti e lo storico delle operazioni effettuate. In particolare, come evidenziato in Figura 4, cliccando sul widget di una specifica categoria di servizio (ad esempio Compute), sarà possibile visualizzare direttamente, secondo le metriche della convenzione, il dettaglio delle quantità totali delle risorse acquistate, quelle già utilizzate e le quantità ancora disponibili. Inoltre, accedendo al menu del profilo presente nell'header dell'interfaccia della Console Unica, il referente dell'Amministrazione avrà la possibilità di impostare gli indirizzi e-mail a cui inviare tutte le notifiche previste nella sezione Messaggi e selezionare altre impostazioni di base (lingua, ecc.).

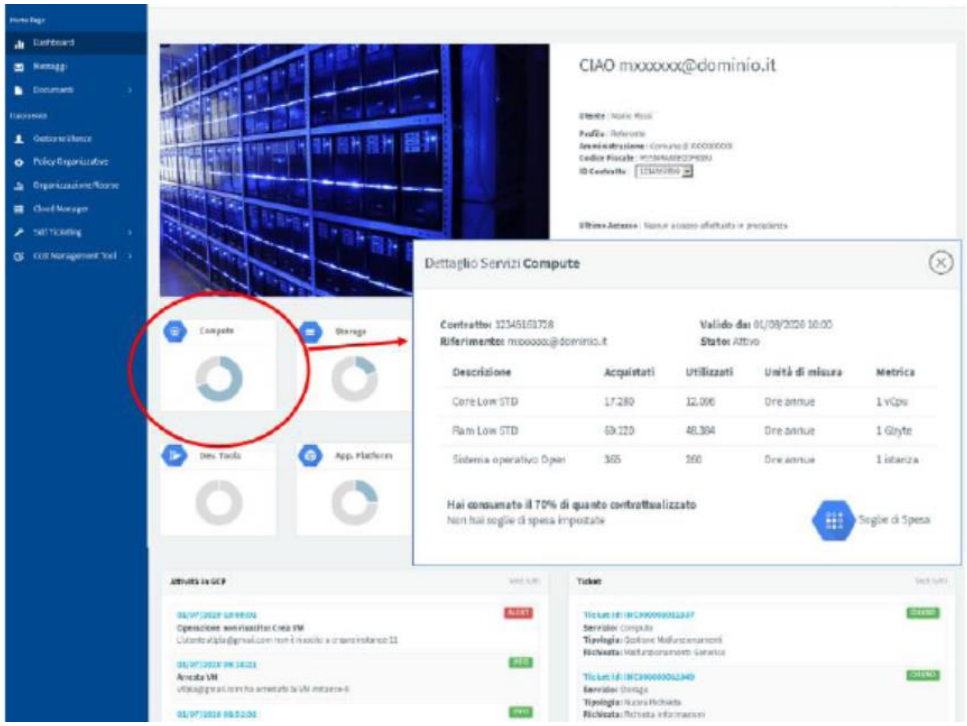



Figura 3 – Dashboard CU

• **Cloud Manager**: in questa sezione, per tutti i servizi della convenzione, ciascuna Amministrazione potrà, nell'ambito della funzione di **Design & Delivery**:

- ✓ costruire l'architettura cloud di ciascun Project all'interno del proprio tenant;
- ✓ attivare i servizi in self-provisioning;

nell'ambito della funzione di **Management & Monitoring**:

- ✓ effettuare operazioni di scale up e scale down sui servizi contrattualizzati;
- ✓ gestire e monitorare tali servizi accedendo direttamente all'opportuna sezione della console. Ogni operazione effettuata sulle console verticali GCP sarà ricondotta nella Console Unica dal modulo Event Detector per l'allineamento delle configurazioni delle risorse contrattualizzate.

Dettagliando ulteriormente la sezione di **Design & Delivery**, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di definire e configurare le risorse cloud contrattualizzate in modalità semplificata ed aderente ai requisiti e alla classificazione dei servizi della Convenzione, garantendo massima autonomia e tempestività nell'attivazione.
Il referente dell'Amministrazione, accedendo dalla sezione "I tuoi servizi" alla dashboard del Cloud Manager potrà nella fase di **Design & Delivery**:

- ***selezionare***, utilizzando l'apposito menu a tendina presente nell'header della pagina, un Project tra quelli esistenti;
- ***visualizzare*** sia le categorie di servizio in cui sono state attivate risorse con il relativo dettaglio (identificativo della risorsa) sia quelle che non hanno risorse istanziate ;
- ***istanziare*** in modo semplificato, per ciascuna categoria di servizi della Convenzione, attraverso la funzionalità "Configura", nuove risorse cloud utilizzando una procedura guidata che espone

solo le funzionalità base per l'attivazione delle risorse cloud garantendo velocità di esecuzione. Nel caso in cui l'Amministrazione voglia, invece, utilizzare tutte le funzionalità di configurazione del Cloud Manager potrà accedervi direttamente dal tasto "Funzionalità Avanzate" presente in ciascuna finestra di configurazione.
- ***monitorare***, in fase di attivazione delle risorse, lo stato di avanzamento dei consumi per la specifica categoria di servizi nel Project selezionato in modo da avere sempre a disposizione una vista delle quantità disponibili e in uso.

Dettagliando ulteriormente la sezione di **Management & Monitoring**, dopo aver terminato la fase di attivazione delle risorse cloud all'interno del Project selezionato, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di:
- ***gestire la singola risorsa*** accedendo direttamente alle specifiche funzionalità presenti console tramite il button "Gestisci";
- ***monitorare le performance*** della risorsa accedendo alle funzionalità di monitoraggio tramite il relativo button "Monitora".

In alternativa, il referente dell'Amministrazione ha la possibilità di accedere alle funzionalità avanzate della dashboard tramite il relativo button "presente nell'header della sezione.

## 2.3 Gestione e Monitoraggio

La struttura sarà organizzata in turni di lavoro continuativi su 24 ore ed avrà la responsabilità delle seguenti attività:

- fornire la disponibilità degli ambienti preposti all'erogazione del servizio;
- controllare l'esecuzione delle procedure schedulate negli ambienti ambito del servizio;
- segnalare e gestire le anomalie ed i malfunzionamenti di procedure, sistemi e hardware;
- gestire le attività di backup e relativi media;
- gestire gli ambienti ed eseguire il monitoraggio del servizio in relazione agli SLA contrattualizzati con i clienti;
- mantenere la documentazione inerente la gestione operativa dei Data Center;
- eseguire e controllare i processi relativi alla gestione operativa dei Data Center.

Rappresenterà il punto primario di raccolta di tutte le segnalazioni relative ad anomalie e richieste di servizio che incidono sulla qualità e/o disponibilità dei servizi erogati e garantirà la tracciabilità e il monitoraggio di tutte le richieste di assistenza, delle soluzioni e dei passi eseguiti per raggiungere la soluzione mediante il sistema di trouble ticketing.

La struttura utilizzerà appositi strumenti e monitor di controllo del processo di erogazione dell'assistenza che serviranno per verificare e gestire:

- solleciti o reclami del Cliente;
- escalation interne (riassegnazioni fra gruppi diversi);
- riaperture dei ticket da parte del Cliente.

### 2.3.1 Gestione SW Infrastrutturale

Il Servizio prevede l'aggiornamento del Software Infrastrutturale in termini di installazione delle ultime versioni compatibili con l'infrastruttura applicativa oggetto della Fornitura descritta nel documento "*Progetto di Fattibilità*".

### 2.3.2 Gestione SW Operativo

Il Servizio prevede l'aggiornamento del Software in termini di installazione delle ultime versioni compatibili con l'infrastruttura applicativa oggetto della Fornitura descritta nel documento "*Progetto di Fattibilità*".

### 2.3.3 Gestione HW

All'interno del presente Servizio è ricompresa ogni prestazione e attività atta a garantire la continuità, la piena funzionalità e l'efficienza dell'Hardware presente nel Centro Servizio della NewCo PSN, nel rispetto dei requisiti descritti nei paragrafi ***3.4.1 Componente Server*** e ***3.4.2 Componente Storage*** *del documento "Progetto di Fattibilità"*.

### 2.3.4 Modalità di esecuzione dei servizi e delle attività

Le attività oggetto del presente servizio comprendono:

- attività di tipo **continuativo**, remunerate attraverso la corresponsione di un canone mensile;
- attività "**a corpo**", remunerate attraverso la corresponsione di un importo *una tantum* relativo alla valorizzazione dell'attività / servizio erogato.

La tabella seguente riporta – in funzione dei servizi e delle attività illustrate ai precedenti paragrafi – le modalità con cui queste dovranno essere eseguite e le modalità con cui verranno remunerate.

| Servizio | Modalità di erogazione | Modalità di remunerazione | Descrizione di dettaglio | Elementi dimensionali del Servizio |
|---|---|---|---|---|
| **Housing** | Continuativa | Canone mensile per ciascun rack | Il canone sarà calcolato sulla base del numero di rack delle PAC ospitate in Housing presso i Data Center della NewCo PSN | Housing Dedicato, nelle quantità richieste dalla PAC |
| **Hosting** | Continuativa | Canone mensile per ciascun rack | Il canone sarà calcolato sulla base del numero di rack delle PAC ospitate in Hosting presso i Data Center della NewCo PSN | Hosting Dedicato, nelle quantità richieste dalla PAC |
| **Private IaaS** | Continuativa | Canone mensile per lama fisica | Il canone sarà calcolato sulla base del numero di lame fisiche | Private IaaS, nelle quantità richieste dalla PAC |

| Servizio | Modalità di erogazione | Modalità di remunerazione | Descrizione di dettaglio | Elementi dimensionali del Servizio |
|---|---|---|---|---|
| | | | ospitate presso i Data Center della NewCo PSN | |
| **Shared IaaS** | Continuativa | Canone mensile per VM | Il canone sarà calcolato sulla base del numero di VM delle PAC ospitate in Iaas presso i Data Center della NewCo PSN | Shared IaaS, nelle quantità richieste dalla PAC |
| **PaaS** | Continuativa | Canone mensile per istanza | Il canone sarà calcolato sulla base del numero delle istanze delle PAC ospitate in Paas presso i Data Center della NewCo PSN | PaaS, nelle quantità richieste dalla PAC |
| **CaaS** | Continuativa | Canone mensile per istanza | Il canone sarà calcolato sulla base del numero delle istanze delle PAC ospitate in Caas presso i Data Center della NewCo PSN | CaaS, nelle quantità richieste dalla PAC |
| **Gestione della Sicurezza IT (SOC)** | Continuativa | Canone mensile | La quota di tale canone è inclusa nel canone relativo al servizio Infrastrutturale prescelto | Vedi specifiche indicate al paragrafo 3.3.3 del documento "Progetto di Fattibilità" |
| **Continuità Operativa** | Continuativa | Canone mensile | La quota di tale canone è inclusa nel canone relativo al servizio Infrastrutturale prescelto | Vedi specifiche indicate al paragrafo 2.1 Continuità Operativa |
| **Assistenza e Manutenzione** | Continuativa | Canone mensile | La quota di tale canone è inclusa nel canone relativo al servizio Infrastrutturale prescelto | Vedi specifiche indicate al paragrafo 2.5 Servizio di Assistenza e Manutenzione |
| **Migrazione** | A corpo | Canone Mensile | La quota di tale attività a corpo è distribuita (sommandosi) nel | Vedi specifiche indicate al paragrafo 2.12.2 del documento |

| Servizio | Modalità di erogazione | Modalità di remunerazione | Descrizione di dettaglio | Elementi dimensionali del Servizio |
|---|---|---|---|---|
| | | | canone relativo al servizio prescelto | "Progetto di Fattibilità" |
| **Commissioning / Decommissioning** | A corpo | Una tantum | La quota una tantum relativa all'attività sarà calcolata sulla base della tipologia di servizio richiesto. | |
| **Console Unica di gestione** | Continuativa | Compresa nel servizio | | |

Con cadenza semestrale, le PAC comunicheranno alla NewCo PSN il **Piano di Evoluzione** del proprio Data Center nel semestre successivo, evidenziando l'eventuale necessità di modificare – in aggiunta o in diminuzione – qualsiasi elemento di servizio indicato nel Contratto in essere.

In caso di commissioning, il termine entro il quale la NewCo PSN provvederà alla pianificazione delle attività necessarie non potrà essere superiore a 5 gg lavorativi.

In caso di richiesta di decommissioning di servizi esistenti, il termine entro il quale la NewCo PSN provvederà alla pianificazione delle attività necessarie non potrà essere superiore a 3 gg lavorativi. Sono intese a carico della PA le successive attività di rimozione fisica e trasporto del rack dismesso in altro sito qualora il servizio esistente da dismettere sia l'Housing.

La NewCo PSN si rende disponibile ad effettuare quanto indicato nel Piano di Evoluzione entro 30 giorni dalla comunicazione del piano stesso da parte delle PAC.

### 2.3.5 Collaudi e verifiche di conformità

Le verifiche di conformità verranno effettuate secondo le seguenti tempistiche:

a) A conclusione delle attività di Migrazione, come indicato nel "Progetto di Fattibilità":
b) In corso di esecuzione del contratto, una tantum, con riferimento ad attività "a corpo"
c) Trimestralmente, ai fini della fatturazione.

Durante suddette operazioni, la NewCo PSN supporterà la PAC nell'esecuzione delle prove atte a verificare la conformità delle caratteristiche del servizio nel suo complesso in relazione alle specifiche contenute nel Contratto, nel presente Progetto di Fattibilità. Il supporto alle suddette attività è obbligatorio ed il relativo costo è da intendersi compreso nel prezzo complessivo dei Servizi.

Entro 20 giorni dall'approvazione del Piano di Erogazione dei Servizi da parte della PAC, la NewCo PSN consegnerà alla PAC un documento intitolato "Specifiche di dettaglio delle prove di verifica di conformità" che descriva la tipologia delle prove previste, le modalità con cui verranno eseguite e la pianificazione temporale delle stesse.

Entro 10 giorni dalla ricezione delle suddette specifiche, il Referente della PAC comunicherà alla NewCo PSN eventuali modifiche e/o integrazioni delle stesse. Nei successivi 10 giorni la NewCo PSN predisporrà ed invierà al Referente della PAC un documento definitivo che recepisca le modifiche ed integrazioni formulate da quest'ultima. Tale documento, una volta accettato dal Referente della PAC costituirà la "Guida Operativa" della Commissione di Verifica.

A partire dall'accettazione del documento di "Specifiche di dettaglio delle prove di verifica di conformità" da parte della PAC la NewCo PSN si renderà disponibile ad avviare le attività di verifica secondo le modalità e le tempistiche indicate nel documento.

Le attività avranno inizio a conclusione delle attività propedeutiche all'avvio dei Servizi richiesti.

La NewCo PSN si impegna altresì, qualora richiesto dalla PAC, a svolgere ulteriori prove integrative rispetto a quelle indicate nel documento di cui sopra.

La PAC si riserva di effettuare attività di verifica sui servizi anche nel corso del contratto, con l'obiettivo di accertare la permanenza dei requisiti richiesti.

In caso di esito negativo della verifica di conformità, la NewCo PSN procederà ad ogni attività necessaria all'eliminazione dei malfunzionamenti e sostituzioni di parti e comunicare la disponibilità alla seconda verifica entro il termine perentorio di 10 giorni decorrenti dalla data del verbale di esito negativo della prima verifica di conformità, pena l'applicazione delle relative penali.

Qualora anche la seconda verifica abbia esito negativo verranno applicate le penali riportate nello schema di contratto.

È facoltà delle PA procedere ad ulteriori verifiche ovvero dichiarare risolto il contratto. In tale ultimo caso, la NewCo PSN avrà l'obbligo – a propria cura e spese – di spostare le infrastrutture IT e TLC della PA nel sito indicato dalla PA stessa ed entro il termine che verranno indicati dalla stessa nel provvedimento di risoluzione.

Tutte le attività di verifica dovranno concludersi con la stesura di un "verbale di verifica di conformità". Nel caso di esito positivo, la data del "Verbale positivo di verifica di conformità" avrà valore di "Data di accettazione del servizio".

## 2.4 Security Management

### 2.4.1 Modello di servizio DDOS

Il servizio permette di analizzare e eventualmente mitigare attacchi DDoS su un volume di traffico Cliente fino a 160 Gbps, assicurando all'Amministrazione la riconsegna del traffico lecito per il taglio di banda contrattualizzato.

La scelta del profilo di banda Internet riconsegnata dipende dal volume medio di traffico sviluppato per l'utilizzo dei servizi esposti su Internet.

Qualora l'Amministrazione necessiti di un valore di banda riconsegnata maggiore di quelli indicati verrà valutata la fattibilità del servizio a progetto.

Il servizio DDoS Protection proposto dalla NewCo PSN è caratterizzato inoltre dai seguenti elementi:

- Mitigations: illimitate.
- Tipologia Mitigazione: Il SOC della NewCo PSN eroga il servizio di monitoring costante e al superamento di soglie preimpostate come critiche, la piattaforma attiva e disattiva automaticamente la Diversion, inviando mail automatiche al Richiedente ad ogni cambio di stato della configurazione.
- Durata Attacco: illimitata, ovvero non c'è un limite temporale per la durata della fase di "Diversion".
- Incident Report: entro 2 giorni lavorativi dalla disabilitazione del servizio DDoS Protection.

- Security Operation Center (SOC): presso di esso operano operatori specializzati che si occupano di analizzare gli attacchi ed attivare la "Diversion" del traffico. Il SOC sarà operativo H24/365.

## 2.5 Servizio di Assistenza e Manutenzione

Si intendono a totale carico della NewCo PSN i servizi di Assistenza e Manutenzione degli impianti tecnologici infrastrutturali dei Data Center e delle componenti edili ad essi relativi al Centro Servizi della NewCo PSN. La NewCo PSN si farà carico di tutte le attività di progettazione e set up dei Servizi di Assistenza e Manutenzione, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

In particolare, la **manutenzione** dei servizi comprende l'insieme di operazioni e procedure necessarie al mantenimento della loro corretta funzionalità, efficienza e prestazioni e quindi concorre in maniera determinante al mantenimento dei livelli di servizio concordati e sottoscritti.

L'**ambito** di pertinenza della manutenzione dipende dalla tipologia di servizio in oggetto: ad esempio, in ambito Infrastructure-as-a-Service (IaaS) gli interventi di manutenzione si applicano alle infrastrutture hardware e sistemistiche, che sono l'oggetto del servizio, mentre in ambito Platform-as-a-Service (PaaS) gli interventi si estenderanno alle piattaforme middleware e software, oggetto dello specifico servizio.

Il **perimetro** su cui si estende la manutenzione dipende dalla tipologia di intervento necessario: alcuni interventi di manutenzione possono riguardare servizi sottoscritti da singole Amministrazioni o da ristretti gruppi, altri potrebbero avere un impatto più generalizzato sull'utenza (es. interventi su server room) che in generale proprio per tale motivo sono più rari e di carattere eccezionale.

Le attività di manutenzione possono essere classificate secondo una prima dimensione che rende conto della **tempistica di intervento rispetto al malfunzionamento o al degrado dei livelli di servizio**, che siano potenzialmente previsti o effettivamente in essere:

- **Manutenzione correttiva**, "incidentale": interviene solo all'effettivo manifestarsi del guasto o del degrado del servizio, e quindi attiene a tutti quegli eventi che non sono in alcun modo predicibili, neanche tramite analisi statistiche dei dati di monitoraggio; questo tipo di manutenzione ha quindi per definizione come oggetto interventi urgenti (ma non necessariamente critici e prioritari), che possono anche essere risolti tramite interventi temporanei (workaround), gestiti ad esempio attraverso i processi di Incident e Problem Management delle pratiche ITIL.

- **Manutenzione preventiva**, "programmata": anticipa potenziali malfunzionamenti, degradi dei livelli di servizio o esposizione a rischi di sicurezza, sulla base delle correzioni suggerite o raccomandate dai vendor tecnologici (es. patching sistemistici), oppure sulla base dell'analisi di metriche anticipatrici note, rilevate tramite i sistemi di monitoraggio e analizzate dai team preposti. L'analisi di questi dati insieme alle informazioni ed alla conoscenza del ciclo di vita dei servizi erogati, permette di ottimizzare gli interventi manutentivi al fine di prevenire rischi e malfunzionamenti. Questo tipo di interventi anticipa dunque la problematica, che rimane solo potenziale, ed è programmato sulla base dell'urgenza dell'intervento stesso (stabilita ad esempio sulla base delle potenziali conseguenze).

- **Manutenzione predittiva**, "programmabile": è sostanzialmente analoga alla manutenzione preventiva nella tempistica di intervento, in quanto essa anticipa potenziali eventi di malfunzionamento o degrado dei servizi, tuttavia ciò non avviene sulla base del ciclo di vita noto dei servizi o sulle raccomandazioni pubblicate dai vendor, nè su metriche anticipatrici note, bensì viene intercettata sulla base di un approccio di analisi dinamica (*real-time*) e incrociata di diverse metriche monitorate, supportata da funzioni di analisi predittiva che si avvalgono di algoritmi di Machine Learning in grado di

individuare predittori di malfunzionamenti. Da tali caratteristiche discende che la manutenzione predittiva è certamente programmabile, ma non programmata a priori. Gli strumenti di Data Mining e di Machine Learning, che consentono la modellazione predittiva, vengono messi a disposizione di funzioni di AI-ops (*Artificial Intelligence for Operations*), e costituiscono alcuni degli strumenti a supporto utilizzati per realizzare questo specifico ambito di manutenzione.

Infine, gli interventi di manutenzione possono essere classificati sulla base di una seconda dimensione che ne individua la **priorità di intervento**.

Si definisce così la "**manutenzione ordinaria**" quella che ha per oggetto interventi non prioritari, che possono quindi essere preventivamente concordati e pianificati successivamente (ciò vale anche per interventi di manutenzione correttiva, che sebbene siano incidentali, possono essere comunque posticipati e quindi pianificabili, non essendo critici) o che comunque possono essere ricondotti alle finestre di tempo periodiche predefinite.

Si definisce infine la "**manutenzione straordinaria**" quella che ha per oggetto interventi prioritari e non procrastinabili, nell'ambito della quale ricadono quindi eventi ritenuti critici per l'erogazione corretta e sicura dei servizi. Tali interventi non possono essere dunque posticipati e hanno un carattere emergenziale, per cui devono essere realizzati entro il più breve tempo possibile: per questo motivo, tali interventi ricorrono a finestre di intervento straordinarie e non preventivamente pianificate, ancorché comunicate in anticipo alle Amministrazioni coinvolte.

### 2.5.1 Centro di Gestione

La NewCo PSN renderà disponibile una **soluzione organizzativa** basata su un **Centro Servizi Virtuale**, **distribuito su più centri (Control Room), attivo e presidiato in modalità continuativa (H24x7) da personale qualificato e certificato operativo in lingua italiana**.
Il Centro Servizi virtuale sarà distribuito sul territorio nazionale su più sedi per garantire la massima affidabilità e flessibilità nella gestione dei servizi previsti ed organizzato in almeno un Centro Servizi **Primario** ed uno **Secondario**. I due Centri Servizi saranno posizionati sul territorio italiano ad una distanza di almeno 500 km così da garantire la continuità operativa in caso di indisponibilità del Centro Primario dovuta a disastro geografico. Il Centro Servizi Secondario sarà immediatamente operativo perché potrà contare sia su un processo di formazione continua sia su una Knowledge Base condivisa. Entrambi i Centri Servizi individuati dalla NewCo PSN sono certificati UNI CEI ISO/IEC 27001: 2017.

La NewCo PSN assicura tale servizio in conformità ai Servizi elencati al ***capitolo 2 Servizi Offerti e Modalità di Erogazione*** ed ai Requisiti espressi al ***capitolo 3 Sicurezza capitolo 4 Infrastruttura IT e Network*** *del documento "Progetto di Fattibilità"*.

### 2.5.2 Servizio di Contact Center

La NewCo PSN erogherà un servizio di Contact Center, informativo e di gestione e manutenzione, strutturato in modo da indirizzare adeguatamente le richieste di ogni singola Amministrazione Contraente in modo specifico e contestualizzato. Il Contact Center sarà accessibile attraverso un'infrastruttura multicanale, in grado di gestire i contatti in modo unificato e omogeneo. I diversi canali di accesso disponibili dovranno essere:

- numero verde dedicato per le chiamate telefoniche;
- numero telefonico dedicato per la ricezione dei fax;

- indirizzo e-mail dedicato;
- portale web per l'apertura e monitoraggio dei ticket – Trouble Ticketing System (TTS)

Tutti i canali saranno integrati in un modello unico di trattamento, in cui le segnalazioni vengono indirizzate a diversi gruppi specializzati di operatori utilizzando le corrette politiche di instradamento. La figura seguente rappresenta lo schema organizzativo generale che avrà il Contact Center e le interazioni con le altre strutture della NewCo PSN coinvolte nei processi di gestione e manutenzione.

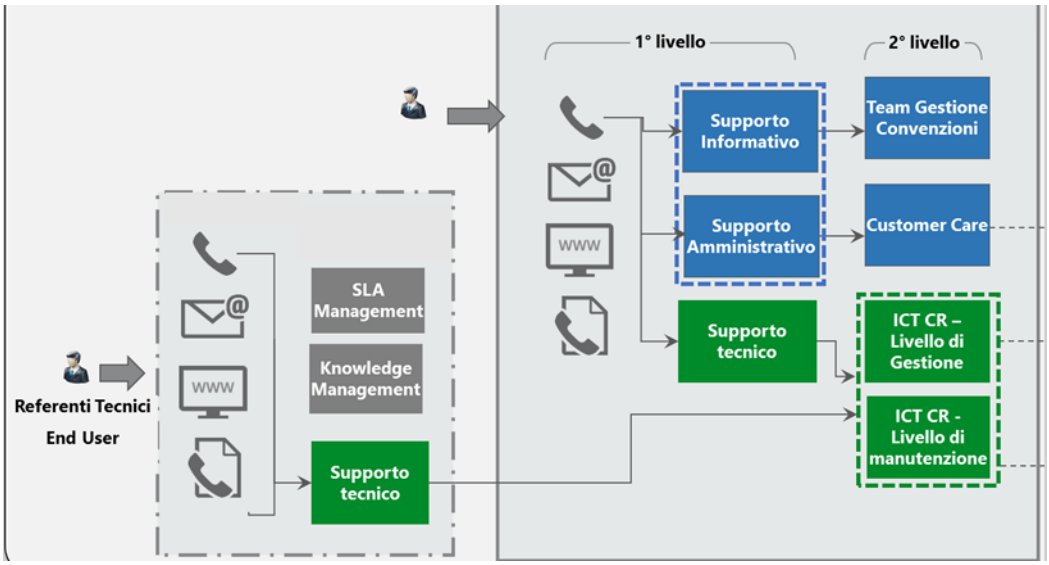



*Figura 4 - Esempio organizzazione Contact Center*

Il servizio sarà articolato su due livelli logici, entrambi in grado di soddisfare:

1. richieste di tipo **informativo**, provenienti da Amministrazioni che ancora non hanno aderito alla convenzione, volte ad ottenere informazioni sui servizi in prospettiva di una sottoscrizione;
2. richieste di tipo **amministrativo**, provenienti da Amministrazioni già contraenti, su aspetti legati alla conduzione del contratto (ad es. fatturazione dei servizi);
3. richieste di tipo **tecnico**, provenienti da Amministrazioni che desiderano segnalare un disservizio, richiedere attività di gestione e manutenzione.

L'accesso per le richieste di **tipo 1** dovrà esser reso disponibile a tutte le Amministrazioni, mentre per quelle di **tipo 2 e 3** dovrà esser richiesto un PIN di riconoscimento, che verrà assegnato alle Amministrazioni alla stipula del contratto.

La struttura resa disponibile sarà completata da una funzione di Knowledge Management, che alimenterà la Knowledge Base (repository alimentato in modo incrementale, in cui gli operatori del Service Desk possono memorizzare soluzioni per risolvere richieste ricorrenti o ripetibili) del servizio sulla base delle segnalazioni ricevute.

#### 2.5.2.1 Trouble Ticketing System

Indipendentemente dal canale di accesso utilizzato, tutte le richieste pervenute all'Help Desk saranno tracciate attraverso il TTS, in grado di registrare almeno le seguenti informazioni minime:

- codice identificativo del (TT);

- descrizione della segnalazione (segnalazione di disservizio; richiesta accesso locali; sollecito; reclamo);
- modalità di ricezione (telefono, fax, mail, web);
- data e orario di apertura TT;
- referente della PA che ha contattato l'Help Desk;
- stato del TT;
- descrizione della azione intrapresa;
- diagnosi del disservizio, ove applicabile;
- data e orario di chiusura.

L'attivazione del servizio di Help Desk tecnico sarà contestuale alla presa in carico dei servizi sottoscritti dalla singola PA.

## 2.6 Service Management

Questa struttura rappresenterà l'interfaccia della NewCo PSN nei confronti del Cliente per tutti gli aspetti relativi all'erogazione del Servizio e alla gestione dei rapporti e delle relazioni operative, nell'ambito di quanto definito dal Contratto.

Periodicamente (e.g. ogni 2 mesi) saranno pianificati incontri tra tale struttura e la corrispettiva della PA per verificare l'andamento del servizio stesso e valutare eventuali richieste di variazione.

La NewCo PSN dettaglierà il presente Servizio all'interno di un documento di **Governance** complessiva del rapporto con le PAC; tale documento rappresenterà le modalità operative da mettere in campo all'atto della sottoscrizione del contratto tra le PAC ed il PSN. Il documento dovrà essere conforme agli standard di mercato applicabili (ad esempio ITIL Framework).

La NewCo PSN presenterà tale documento sin dalla data di presentazione dell'offerta, e dovrà garantire per tutta la durata della Fornitura, un aggiornamento costante, oltre ad offrire un continuo miglioramento dei processi attuati e un utilizzo ottimale delle risorse impiegate.

## 2.7 SLA Management

I Service Level Agreement (SLA) definiscono i parametri di qualità del servizio che devono essere rispettati dalla NewCo PSN. La finestra temporale di erogazione dell'intero servizio è 24H (00:00 – 24:00) per 365 giorni l'anno.
Per il dettaglio dei Service Level Agreement si faccia riferimento al documento "*Allegato 01 - Indicatori di Qualità*".

### 2.7.1 Calendario degli interventi

Le due parti (Amministrazione e NewCo PSN) condividono gli interventi rilevanti attraverso il cosiddetto "**Availability Calendar**", che definisce le finestre in cui saranno eseguite le attività che possono impattare sulla qualità dei servizi (quali ad esempio adeguamenti infrastrutturali, vulnerability test, etc..).

L'Availability Calendar indica anche le finestre target per l'esecuzione delle attività di commisioning e decomissioning, fatte salve migliori intese tra le parti su casi specifici.

All'interno dell'Availability Calendar sono inoltre indicati i cosiddetti frozen period, basati sull'esperienza e le best practice, solitamente previsti nella seconda metà di dicembre, la prima settimana di gennaio, il periodo pasquale e le tre settimane centrali di agosto. I reali frozen period potrebbero variare rispetto a quanto indicato, ma in ogni caso non supereranno i periodi totali definiti.
La "Finestra di Manutenzione Mensile" (FMM) è solitamente pianificata in due momenti mensili, in orario notturno e di una durata massima di 6 ore, così come indicato nell'Availability Calendar, ad esempio il secondo Martedì del mese e il terzo Giovedì del mese, tra le 22:00 e le 4:00. A fronte di possibili variazioni della data di calendario precedentemente comunicata, il Cliente riceverà tempestivamente una comunicazione scritta contenente la nuova data pianificata.

Attività non standard potrebbero verificarsi per interventi sulle infrastrutture, e potrebbero causare una disponibilità limitata del servizio. Queste attività saranno comunicate in anticipo, tenendo in considerazione le richieste fatte dai clienti, indicando:

- ragione dell'attività;
- impatto derivante dall'attività;
- orario di inizio dell'attività;
- durata dell'attività, così come se vi sarà una interruzione parziale e/o totale del servizio;
- tipologia di attività di manutenzione.

Le fasce orarie indicate non concorreranno al processo di misurazione dei Service Level Object (SLO).

Qualora la NewCo PSN identifichi che sussistano giustificati motivi che evidenzino il manifestarsi di gravi danni sui servizi (es. fermo del servizio o condizioni che sono prossime a determinare tale situazione), è autorizzato ad effettuare attività in emergenza, al di fuori delle finestre pianificate. Per le attività eseguite in emergenza non sarà richiesta autorizzazione preventiva all'Amministrazione. La NewCo PSN informerà in anticipo l'Amministrazione riguardo a tale attività ed in coerenza con le procedure definite nell'ambito del processo di Incidenti Management. Inoltre gli eventuali disservizi riconducibili a manutenzioni di emergenza, qualora derivanti da errori/anomalie imputabili alla NewCo PSN, non interromperanno il processo di misurazione degli SLO.

## 2.8 Assicurazione della Qualità

Nell'esecuzione delle attività contrattualmente previste la NewCo PSN si impegna a:

- Rispettare i principi di gestione della qualità della norma EN ISO 9001 rispetto alla quale gli è stata richiesta la certificazione.
- Attenersi ad essere conforme a quanto previsto dal "**Piano di Qualità della Fornitura**".
- Rispettare i principi per il sistema di gestione della sicurezza delle informazioni, della norma ISO IEC 27001:2013.

Il **Piano di Qualità sarà redatto dalla NewCo PSN** e costituirà il riferimento per le attività di verifica e validazione svolte dalla NewCo PSN all'interno dei propri gruppi di lavoro.

Entro 30 (trenta) giorni solari dalla data di stipula del contratto, la NewCo PSN consegnerà alla PA il Piano di Qualità.

Il Piano di Qualità della fornitura, descriverà le modalità realizzative e garantirne l'adeguatezza rispetto agli obiettivi durante tutta la fornitura.

Il Piano di Qualità della fornitura verrà aggiornato a seguito di significativi cambiamenti di contesto in corso d'opera o, comunque, su richiesta della PA ogni qualvolta lo reputi opportuno. In questo caso dovrà

essere riconsegnato l'intero documento, e non per le sole parti variate, e dovrà essere possibile individuare le modifiche effettuate.

Nella stesura del Piano di Qualità della fornitura, la NewCo PSN andrà a dettagliare, per ciascun requisito di qualità, le fonti dati utilizzate per la raccolta dei dati elementari e gli strumenti utilizzati per l'elaborazione delle informazioni di dettaglio.

Le successive versioni o revisioni del Piano di Qualità della fornitura saranno consegnate in funzione delle variazioni intervenute.

### 2.8.1 Audit Qualità

La PA si riserva la facoltà di effettuare audit di qualità presso la NewCo PSN. Tali audit saranno finalizzati a monitorare e verificare che le attività e/o i processi siano svolti dalla NewCo PSN nel rispetto di quanto definito a livello contrattuale; provvede ad organizzare l'audit, predisponendo eventuali check list di supporto, e si accorda con la NewCo PSN in merito alla data di svolgimento delle verifiche ispettive; esegue la verifica ispettiva e a conclusione della stessa redige il verbale di verifica annotando eventuali anomalie riscontrate.

Il verbale di verifica viene inviato dalla PA alla NewCo PSN affinché questi, in conseguenza di eventuali non conformità rilevate, ne individui le cause, definisca tempi e modi delle azioni da intraprendere; la NewCo PSN provvede successivamente ad inviare le proposte delle azioni correttive alla PA per verifica e approvazione.

La PA si riserva, inoltre, la facoltà di richiedere alla NewCo PSN la definizione di azioni correttive, preventive o migliorative, ad esempio in relazione ad eventi notificati in sede di monitoraggio della fornitura o di gestione di rilievi e penali, al fine di incidere sulle cause che hanno generato l'evento notificato ed evitare il ripetersi o il verificarsi di un problema.

### 2.8.2 Audit Sicurezza

La PA ha la facoltà di effettuare audit di sicurezza presso la NewCo PSN. Tali audit saranno finalizzati a monitorare e verificare che le attività e/o i processi siano svolti dalla NewCo PSN nel rispetto di quanto definito a livello contrattuale. In particolare, la NewCo PSN deve:

- accettare visite ispettive da parte della PA o da terze parti designate/incaricate; concordare con gli auditor il contenuto e la tempificazione delle eventuali azioni correttive, preventive, migliorative, porle in atto assicurandone il tracciamento fino alla verifica del buon fine ("chiusura") da parte degli auditor.
- Da parte sua la PA si impegna a raccogliere e valutare motivate proposte migliorative, comunque sottoposte, per il possibile loro recepimento in successive versioni delle politiche di sicurezza.

In particolare, la NewCo PSN è responsabile del corretto utilizzo e gestione, da parte del suo personale, delle credenziali che gli vengono rilasciate per l'accesso ai sistemi della PA.

## 3 Chiusura della Fornitura

La NewCo PSN si impegna, al termine del rapporto contrattuale, a fornire il supporto per il subentro del nuovo gestore della Concessione della Fornitura nel successivo anno mediante il trasferimento delle competenze sulle attività condotte ed il trasferimento dei dati ospitati presso il proprio Centro Servizi al

fine di rendere la prosecuzione delle attività quanto più agevole possibile nel rispetto dagli art. 180 e seguenti del D.Lgs. 18 aprile 2016 n. 50 e smi (Codice Appalti).

# 4 Portale di Fornitura

Per garantire al MITD, agli eventuali organismi di coordinamento e controllo e alle diverse amministrazioni aderenti il monitoraggio e il governo dei Servizi Tecnologici sottoscritti, la NewCo PSN mette a disposizione un portale web, multicanale e raggiungibile tramite Internet, che consente al tempo stesso di promuovere la condivisione e l'esperienza maturata nelle singole iniziative.
Il Portale funge anche da strumento di marketing e promozione per la PA e di comunicazione verso i cittadini e le imprese, offrendo servizi di informazione e monitoraggio circa l'andamento delle varie iniziative.
Il Portale offre dunque una serie di funzionalità e servizi integrati per le aree di comunicazione, informazione, monitoraggio e collaborazione per le PA, ottimizza le caratteristiche di fruibilità degli strumenti e delle sezioni secondo una struttura di navigazione semplice e intuitiva. Per le aree riservate del portale, in cui è richiesto un accesso tramite autenticazione, il Portale offre la possibilità di accedere tramite SPID aderendo alle linee guida di promozione della trasformazione digitale della PA (digital identity only).
Di seguito una mappa concettuale di navigazione del portale:

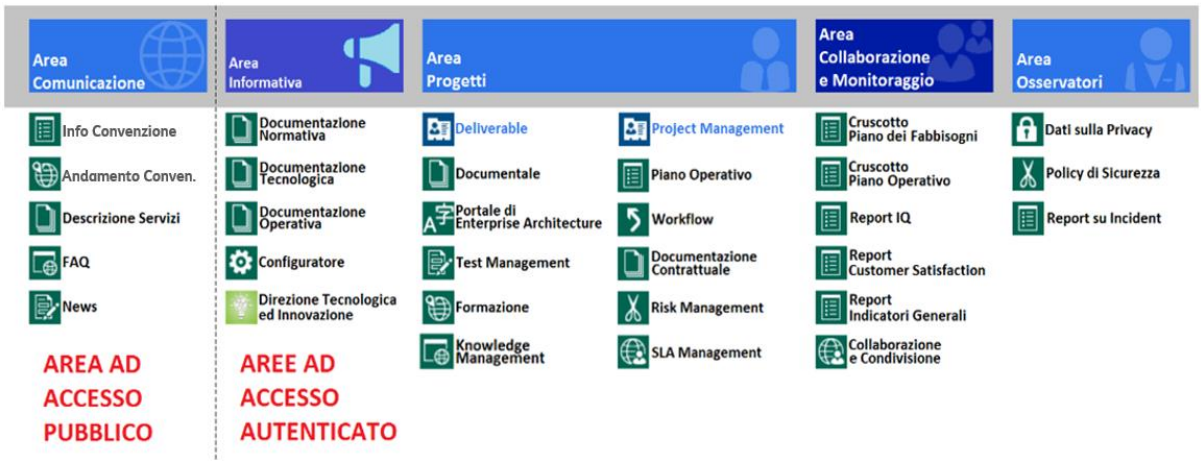



*Figura 5 - Esempio di Mappa di navigazione del Portale*

In cui sono presenti le seguenti aree:

- **Area Comunicazione**: area ad accesso pubblico indicizzata sui motori di ricerca web. Comprende la homepage di portale e fornisce l'accesso alle Informazioni della convenzione, descrizione dei Servizi, FAQ, News. Permette inoltre la consultazione pubblica di una Dashboard dinamica contenente KPI Sintetici complessivi. Nell'area Comunicazione, il Comitato di Cloud Innovation, del RTI cura la pubblicazione degli aggiornamenti tecnologici forniti dalla Direzione Tecnologica ed Innovazione al fine di mantenere allineati e informati gli utenti in merito all'innovazione e strategia tecnologica in atto.
- **Area Informativa**: area ad accesso autenticato destinata alla fruizione di contenuti informativi da parte delle PA. Oltre alla pagina di overview, fornisce l'accesso alla documentazione normativa, tecnologica, operativa ed un utile strumento di orientamento generale che consenta alle Amministrazioni di essere assistite nella scelta degli eventuali servizi da attivare. Attraverso

un sistema di finder e grazie a step progressivi, l'Amministrazione viene guidata nella scelta dei vari servizi. All'interno dell'Area Informativa, oltre alla documentazione sopra citata, viene creata un'apposita sezione aggiuntiva in cui sono resi disponibili tutti i documenti redatti e che potranno esser consultati e/o scaricati dalle Amministrazioni per un aggiornamento sui trend innovativi adottati dal RTI.

- **Area Progetti**: area ad accesso autenticato destinata a tutte le PA registrate (anche in fase precontrattuale) ed al RTI per la consultazione, gestione e collaborazione dei progetti. Presenta una dashboard riepilogativa sui progetti di competenza e fornisce la possibilità di creare nuove istanze di progetto. Per ciascun progetto, tramite l'accesso all'area dedicata, sono offerte tutte le funzionalità di Project Management (tramite strumenti quali Gantt, Workflow, Deliverable, Dashboard e strumenti esterni) per seguire: ✓la **predisposizione** di **richieste** di attivazione di ciascuna iniziativa progettuale da parte dell'Amministrazione, ✓la **pianificazione generale** e di dettaglio per ciascun servizio a carattere progettuale e/o continuativo con il Piano Operativo, il Gantt che riporta tempi e date di consegna , dettaglio dei deliverable previsti e degli effort stimati, il Piano dei rischi, ✓**la gestione del versionamento** dei piani di lavoro, ✓la **rendicontazione e consuntivazione** degli stati di avanzamento lavori e degli SLA, fino alla verifica di conformità finale e conclusione del periodo di garanzia, tramite report e Dashboard di sintesi, ✓**gli strumenti di interazione social** per condividere le esperienze tra i partecipanti. All'interno dell'area Progetti la sezione Deliverable include la gestione documentale che consente, in base a profili utenti e ruoli, di accedere in lettura/scrittura alle aree condivise, distribuire lo spazio documentale in modo differenziato, abilitare il versioning illimitato e/o limitarlo ad un numero di versioni predefinite, etc. Gli utenti tramite un'interfaccia omogenea potranno: ✓**Accedere** al servizio via browser per archiviare, aprire, visualizzare e sincronizzare i propri documenti nello spazio di archiviazione assegnato all'Amministrazione; ✓**Sincronizzare** le raccolte di documenti con le cartelle locali, nella modalità "Drag and drop" ✓**Definire** più siti ovvero aree condivise con gruppi diversi di utenti, con funzioni di check-in/check-out, autorizzazione dei contenuti, versioning, cronologia; ✓**Configurare** la profondità del Versioning, per singolo documento, migliorando il controllo delle modifiche e semplificando la revisione dei contenuti e la contribuzione a più mani sugli stessi file; ✓**Creare** e gestire Wiki, forum, chat e newsletter, per stimolare e facilitare la collaborazione.
- **Area Collaborazione e Monitoraggio**: in cui sono presenti
  - area destinata a tutti gli utenti di Portale che fornisce un ambiente social di interazione tra le parti per lo scambio di contributi compresi quelli non strettamente collegati ad uno specifico progetto. In quest'area convergeranno anche i contenuti social generati sui singoli progetti visualizzabili esclusivamente dai profili autorizzati.
  - area riservata agli utenti MITD/Osservatori, destinata ad accogliere le funzionalità di ricerca, monitoraggio e controllo di progetti, fasi e deliverable dei vari progetti di competenza. Viene fornita una pagina dashboard filtrabile con tutti gli indicatori necessari a fornire una rapida overview sullo stato d'avanzamento, sulle risorse assegnate e sui deliverable prodotti di tutti i progetti. Attraverso l'uso dei filtri sarà possibile scremare i contenuti relativi ad un singolo progetto/fase/deliverable. Comprende inoltre tutte le funzionalità di interrogazione e reportistica mirati alla visualizzazione di Dashboard ed alla generazione di report personalizzati declinati secondo le aspettative del ruolo che l'utente ricopre e focalizzate sui singoli fattori di interesse in termini di indicatori di qualità, di digitalizzazione, gestionali ed economici.
- **Area Osservatori**: area riservata agli utenti MITD/Osservatori, destinata ad accogliere gli strumenti di ricerca, monitoraggio e controllo dei deliverable e dei singoli KPI relativi ai dati di qualità e sicurezza al fine di garantire il corretto svolgimento delle funzioni di monitoraggio della

qualità e della sicurezza. Verrà fornita una dashboard riepilogativa sui parametri di cui sopra ed un motore di ricerca per individuare in maniera puntuale task, documentazione e dati necessari all'espletamento delle proprie responsabilità.

# Proposta per la realizzazione secondo il modello del Partenariato Pubblico Privato del Polo Strategico Nazionale

## Allegato 01 - Indicatori di Qualità

27 settembre 2021

Rev. 1.0

TIM - Uso Interno - Tutti i diritti riservati.

Si riporta nel presente allegato l'elenco dei Service Level Agreement (SLA) proposti per l'erogazione dei servizi oggetto del presente progetto. Per ciascuno dei parametri è stabilito un "Valore di Soglia" ovvero il valore minimo che la NewCo PSN si impegna a garantire
Al superamento del "Valore di Soglia" scatterà il meccanismo di applicazione delle relative penali. Al fine dell'applicazione delle penali saranno considerati i "Valori di Soglia" indicati nella presente "Specificazione delle caratteristiche del Servizio e della Gestione".

Di seguito la tabella di riepilogo, che schematizza la matrice di corrispondenza tra gli Indicatori di Qualità validi per l'intera fornitura, l'ambito di applicazione, la presenza di una azione contrattuale previste nel caso di non rispetto (Penale) e il soggetto verso cui sarà tenuta la rendicontazione:

| Ambito | ID | Descrizione | Penale | Rendicontazione |
|---|---|---|---|---|
| Governo della Fornitura | IQ01 | Invio rendicontazione flussi mensili | Sì | MITD |
| | IQ02 | Invio rendicontazione flussi annuali | Sì | MITD |
| | IQ03 | Rispetto di una scadenza temporale | Sì | Amministrazione |
| | IQ04 | Non approvazione di documenti | Sì | Amministrazione |
| | IQ05 | Attivazione degli interventi | Sì | Amministrazione |
| | IQ06 | Disponibilità degli strumenti di supporto | Sì | Amministrazione |
| Erogazione dei Servizi | IQ07 | Indisponibilità Infrastruttura | Sì | MITD |
| | IQ08 | Disponibilità del servizio di Infrastruttura (Housing) | Sì | Amministrazione |
| | IQ09 | Disponibilità del servizio di Infrastruttura (Hosting) | Sì | Amministrazione |
| | IQ010 | Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS | Sì | Amministrazione |
| | IQ011 | Rispetto dell'RTO | Sì | Amministrazione |
| | IQ012 | Rispetto dell'RPO | Sì | Amministrazione |
| | IQ013 | Rispetto dell'RTO (DR su diversa Region) | Sì | Amministrazione |
| | IQ014 | Rispetto dell'RPO (DR su diversa Region) | Sì | Amministrazione |
| | IQ015 | Disponibilità dei dati a fine fornitura | Sì | Amministrazione |
| Help Desk | IQ016 | Tempo di presa in carico | Sì | Amministrazione |
| | IQ017 | Tempo di risoluzione | Sì | Amministrazione |
| Migrazione | IQ018 | Rispetto dei volumi previsti nel piano di migrazione | Sì | Amministrazione |

## *1 INDICATORI DI QUALITÁ PER IL GOVERNO DELLA FORNITURA*

| **ID** | **IQ01** | **PARAMETRO** | **Invio rendicontazione flussi mensili** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità verifica il ritardo del Fornitore nel produrre e fornire all'Amministrazione i documenti contrattuali della Convenzione nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati | |
| **FORMULA** | | IQ01 = $data_{eff} - data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Mensile | |
| **VALORE DI SOGLIA** | | IQ01 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il MITD applicherà una penale pari ad € 200,00. | |
| **APPLICAZIONE** | | MITD | |

| **ID** | **IQ02** | **PARAMETRO** | **Invio rendicontazione flussi annuali** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità verifica il ritardo del Fornitore nel produrre e fornire all'Amministrazione i documenti contrattuali della Convenzione nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati | |
| **FORMULA** | | IQ02 = $data_{eff} - data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Annuale | |
| **VALORE DI SOGLIA** | | IQ02 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il MITD applicherà una penale pari ad € 500,00. | |
| **APPLICAZIONE** | | MITD | |

| **ID** | **IQ03** | **PARAMETRO** | **Rispetto di una scadenza temporale** |
|---|---|---|---|
| **DESCRIZIONE** | | Per ciascun servizio e per ciascun deliverable prodotto nell'ambito dello stesso, il rispetto di una scadenza stabilita dal contratto e/o indicata nel Progetto di fattibilità | |
| **FORMULA** | | IQ03 = $data_{eff} - data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) | |

| | |
|---|---|
| **FREQUENZA DI MISURAZIONE** | A EVENTO |
| **VALORE DI SOGLIA** | IQ03 ≤ 0 |
| **PENALE** | Per ogni giorno lavorativo eccedente la soglia, l'Amministrazione applicherà la penale pari allo 0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale dell'obiettivo/servizio di riferimento nel contratto esecutivo di fornitura. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ04** | **PARAMETRO** | **Non approvazione di documenti** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore si applica alla mancata approvazione di un documento basilare per le attività progettuali. Sono inderogabilmente basilari i seguenti documenti:<br>• deliverable di fornitura<br>• il Piano di lavoro generale<br>• I verbali di stato di avanzamento lavori – SAL.<br>Nel corso della fornitura l'Amministrazione potrà indicare ulteriori documenti.<br>La fonte dei dati possono essere E-mail, lettere, verbali.<br>Viene definito il parametro "N_rilievi" che verrà incrementato di una unità ogniqualvolta un documento non verrà approvato | |
| **FORMULA** | | IQ04 = N_rilievi<br>Nr di documenti (deliverables) non approvati = N_rilievi + 1 | |
| **FREQUENZA DI MISURAZIONE** | | A semestre | |
| **VALORE DI SOGLIA** | | IQ04 < 5 | |
| **PENALE** | | Il superamento del valore soglia comporterà per ogni documento aggiuntivo rispetto al valore soglia l'applicazione della penale "Non approvazione di documenti" pari a 500€. | |
| **APPLICAZIONE** | | Amministrazione | |

| **ID** | **IQ05** | **PARAMETRO** | **Attivazione degli interventi** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore misura la tempestività di attivazione degli interventi relativi ai servizi professionali a partire dalla richiesta dell'Amministrazione.<br>Viene misurato in giorni lavorativi. | |
| **FORMULA** | | *IQ05 = Data_attiv_int - Data_rich_int*<br>dove per ciascun intervento vanno rilevati - Data della richiesta di attivazione di un intervento (Data_rich_int) - Data di attivazione dell'intervento (Data_attiv_int) | |
| **FREQUENZA DI MISURAZIONE** | | A EVENTO | |

| | |
|---|---|
| **VALORE DI SOGLIA** | Per interventi pianificati nel Piano di Lavoro Generale: IQ05 = 0 negli altri casi: IQ05 <= 5 giorni lavorativi |
| **PENALE** | Per ogni 5 giorni lavorativi o frazione eccedenti il valore di soglia l'Amministrazione applicherà la penale "Ritardo nell'attivazione dell'intervento" pari all'1‰ dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ06** | **PARAMETRO** | **Disponibilità degli strumenti di supporto** |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura la disponibilità degli strumenti di supporto messi a disposizione dell'Amministrazione di seguito elencati, resi disponibili dalla NewCo PSNper l'erogazione dei servizi stessi per l'intera durata contrattuale:<br>• Portale di Governo e Gestione della Fornitura,<br>• Cruscotto sintetico di controllo/monitoraggio della fornitura,<br>• Sistema di Trouble Ticketing,<br>• Sistema di gestione documentale.<br>Il servizio erogato dagli strumenti di supporto si intende indisponibile quando esso viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso della NewCo PSN e della connettività, mancato funzionamento dell'impianto antincendio e di condizionamento, problematiche IT della piattaforma Host, problematiche IT relative al middleware e applicative che inibiscono la completa fruizione del servizio.<br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio erogato dai sistemi di supporto è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |
| **FORMULA** | | Si definisce "disponibilità" del servizio, espressa come valore percentuale:<br>IQ06 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell'ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br>T = 24x60x365-FMM | |

| | | |
|---|---|---|
| **FREQUENZA DI MISURAZIONE** | Annuale | |
| **VALORE DI SOGLIA** | Soglia minima; IQ06 ≥ 99,70% | |
| **PENALE** | L'indisponibilità della infrastruttura a supporto della erogazione dei servizi per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l'emissione di una penale pari al 1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. | |
| **APPLICAZIONE** | Amministrazione | |

## *2 INDICATORI DI QUALITÁ PER L'EROGAZIONE DEI SERVIZI*

| **ID** | **IQ07** | **PARAMETRO** | **Indisponibilità Infrastruttura** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità rappresenta il rispetto della scadenza di messa in esercizio dell'Infrastruttura proposta dal fornitore nei tempi previsti, ossia entro 6 mesi dalla stipula del contratto. | |
| **FORMULA** | | IQ07 = $data_{eff} - data_{prev}$<br>Data prevista di avvio attività (data_prev)<br>Data effettiva di avvio attività (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Ad evento | |
| **VALORE DI SOGLIA** | | IQ07 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il MITD applicherà una penale pari ad € 10.000. | |
| **APPLICAZIONE** | | MITD | |

| **ID** | **IQ08** | **PARAMETRO** | **Disponibilità del servizio di Infrastruttura (Housing)** |
|---|---|---|---|
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità Housing) si intende indisponibile quando l'esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso della NewCo PSN e della connettività, il mancato funzionamento dell'impianto antincendio e di condizionamento e qualunque evento riconducibile alla responsabilità della NewCo PSN.<br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |
| **FORMULA** | | Si definisce "disponibilità" del servizio, espressa come valore percentuale:<br>IQ08 = $(1 - \frac{\sum_{J=1}^{M} d_j}{T}) \times 100$<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell'ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre di Manutenzione Programmata e straordinaria Impianti Data Center (MPSIDC).<br>T = 24x60x365-MPSIDC | |

| | |
|---|---|
| **FREQUENZA DI MISURAZIONE** | Annuale |
| **VALORE DI SOGLIA** | Soglia minima; IQ08 ≥ 99,980% |
| **PENALE** | L'indisponibilità servizi infrastrutturali di Housing per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l'emissione di una penale pari al 1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. |
| **APPLICAZIONE** | Amministrazione |

| | | | |
|---|---|---|---|
| **ID** | **IQ09** | **PARAMETRO** | **Disponibilità del servizio di Infrastruttura (Hosting)** |
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità Hosting) si intende indisponibile quando l'esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso della NewCo PSN e della connettività, mancato funzionamento dell'impianto antincendio e di condizionamento, problematiche IT della piattaforma Host e qualunque altro evento riconducibile alla responsabilità della NewCo PSN.<br><br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br><br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |
| **FORMULA** | | Si definisce "disponibilità" del servizio, espressa come valore percentuale:<br><br>IQ09 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br><br>Dove:<br><br>M = numero totale di disservizi;<br><br>dj = durata, espressa in minuti, del disservizio j-esimo nell'ambito della finestra temporale di erogazione;<br><br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br><br>T = 24x60x365-FMM | |
| **FREQUENZA DI MISURAZIONE** | | Annuale | |
| **VALORE DI SOGLIA** | | Soglia minima: IQ09 ≥ 99.95% | |
| **PENALE** | | L'indisponibilità della infrastruttura a supporto della erogazione dei servizi di Hosting per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l'emissione di una penale pari al 1‰ (uno per | |

| | |
|---|---|
| | mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ010** | **PARAMETRO** | **Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS** |
|---|---|---|---|
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità IaaS, PaaS, BaaS, CaaS) si intende indisponibile quando l'esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso della NewCo PSN e della connettività, mancato funzionamento dell'impianto antincendio e di condizionamento, problematiche IT della piattaforma Host e qualunque altro evento riconducibile alla responsabilità della NewCo PSN.<br><br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br><br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |
| **FORMULA** | | Si definisce "disponibilità" del servizio, espressa come valore percentuale:<br><br>IQ010 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br><br>Dove:<br><br>M = numero totale di disservizi;<br><br>dj = durata, espressa in minuti, del disservizio j-esimo nell'ambito della finestra temporale di erogazione;<br><br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br><br>T = 24x60x365-FMM | |
| **TEMPO MISURAZIONE SLA** | | Annuale | |
| **VALORE DI SOGLIA** | | Soglia minima: IQ010 ≥ 99.95% | |
| **PENALE** | | L'indisponibilità della infrastruttura IaaS, PaaS, BaaS, CaaS per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l'emissione di una penale pari al 1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. | |
| **APPLICAZIONE** | | Amministrazione | |
| **ID** | **IQ011** | **PARAMETRO** | **Rispetto dell'RTO** |

| | |
|---|---|
| **DESCRIZIONE** | Il presente indicatore di qualità misura il rispetto del RTO (Recovery Time Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili alla NewCo PSN. Il valore target è 30 minuti. |
| **FORMULA** | IQ011 = (RTO_effettivo - RTO_atteso)<br>dove RTO_atteso = 30 minuti |
| **FREQUENZA DI MISURAZIONE** | Ad evento |
| **VALORE DI SOGLIA** | Soglia minima: IQ011 <= 0 |
| **PENALI** | Per ogni minuto eccedente la soglia, l'Amministrazione applicherà la penale pari all'0,1‰ (zerovirgolauno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ012** | **PARAMETRO** | **Rispetto dell'RPO** |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura il rispetto del RPO (Recovery Point Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al Fornitore.<br>Valore di RPO rappresenta la perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario.<br>Il valore target è 1 minuto. | |
| **FORMULA** | | IQ012 = $\frac{N_C - N_{CFuoriSoglia}}{N_C}$ x 100<br>dove:<br>$N_C$ = Numero di campionamenti = 104 (2 campionamenti a settimana)<br>$N_{CFuoriSoglia}$ = Numero dei campioni per cui il valore si discosta dal valore soglia | |
| **FREQUENZA DI MISURAZIONE** | | Campionamento effettuato due volte a settimana.<br>SLA su base annuale | |
| **VALORE DI SOGLIA** | | Soglia minima: IQ012 ≥ 99% | |
| **PENALI** | | Per ogni 1% (uno per cento) di scostamento dalla soglia definita, nonché per ogni caso di verificata inconsistenza dei dati di replica, l'Amministrazione applicherà una penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | | Amministrazione | |

| **ID** | **IQ013** | **PARAMETRO** | **Rispetto dell'RTO su diversa Region** |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura il rispetto del RTO (Recovery Time Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili alla NewCo PSN. Il valore target è 4 ore. | |
| **FORMULA** | | IQ013 = (RTO_effettivo - RTO_atteso) | |

| | |
|---|---|
| | dove RTO_atteso = 4 ore |
| **FREQUENZA DI MISURAZIONE** | Ad evento |
| **VALORE DI SOGLIA** | Soglia minima; IQ013 ≤ 0 |
| **PENALI** | Per ogni ora solare eccedente la soglia, l'Amministrazione applicherà la penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ014** | **PARAMETRO** | **Rispetto dell'RPO su diversa Region** |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura il rispetto del RPO (Recovery Point Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al Fornitore.<br>Valore di RPO rappresenta la perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario.<br>Il valore target è 30 minuti | |
| **FORMULA** | | IQ014 = $\frac{N_C - N_{CFuoriSoglia}}{N_C}$ x 100<br>dove:<br>$N_C$ = Numero di campionamenti = 104 (2 campionamenti a settimana)<br>$N_{CFuoriSoglia}$ = Numero dei campioni per cui il valore si discosta dal valore soglia | |
| **FREQUENZA DI MISURAZIONE** | | Campionamento effettuato due volte a settimana.<br>SLA su base annuale. | |
| **VALORE DI SOGLIA** | | Soglia minima; IQ014 ≥ 99% | |
| **PENALI** | | Per ogni 1% (uno per cento) di scostamento dalla soglia definita, nonché per ogni caso di verificata inconsistenza dei dati di replica, l'Amministrazione applicherà una penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | | Amministrazione | |

| **ID** | **IQ15** | **PARAMETRO** | **Disponibilità dei dati a fine fornitura** |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità monitora il rispetto della scadenza di consegna/riconsegna dei principali deliverable e oggetti della fornitura (es. almeno i dati memorizzati nei DB, file di configurazione, immagine server etc …) stabilita dal contratto e/o dal piano di lavoro approvato, con indicazione della data di fine fornitura.<br>In particolare, l'indicatore riguarda la disponibilità verso l'Amministrazione dei dati conservati/configurazioni nell'ambito dei Centri Servizi alla fine della fornitura della singola componente di servizio. | |
| **FORMULA** | | IQ15 = data_eff - data_ prev | |

| | | |
|---|---|---|
| | dove:<br>data_prev = Data prevista di consegna/riconsegna (concordata con l'Amministrazione)<br>data_eff = Data effettiva di consegna/riconsegna | |
| **FREQUENZA DI MISURAZIONE** | A Evento | |
| **VALORE DI SOGLIA** | Soglia minima: IQ015 ≤ 0 | |
| **PENALI** | Per ogni giorno lavorativo eccedente la soglia, l'Amministrazione contraente applicherà la penale pari all'0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | Amministrazione | |

## *3 INDICATORI DI QUALITÁ PER L'HELP DESK*

| **ID** | **IQ016** | **PARAMETRO** | **Tempo di presa in carico** |
|---|---|---|---|
| **DESCRIZIONE** | | Tempestività di presa in carico delle richieste multicanale ricevute da parte dell'Help Desk e relative ad anomalie e/o richiesta di accesso al Data Center.<br>Tempo, misurato in minuti, intercorrente tra la richiesta e la presa in carico della stessa coincidente con l'apertura del ticket da parte dell'help desk.<br>Il periodo di riferimento per la rilevazione dell'indicatore è pari a 3 mesi.<br>Il valore target è 10 minuti | |
| **FORMULA** | | IQ016= $\frac{N_{richiesta_{presaincarico}\,(T_{presaincarico} \leq 10\ \mathrm{min})}}{N_{richieste}}$ x 100<br>Dove:<br>T_presaincarico = Data_presaincarico_ric – Data_invio_ric<br>Data_invio_ric = Data ora (hh/mm/ss) dell'invio della richiesta<br>Data_presaincarico_ric = Data ora (hh/mm/ss) della effettiva presa in carico della richiesta<br>Numero di richiesta prese in carico (N_richiesta_presaincarico)<br>Numero totale di richieste (N_richieste) | |
| **FREQUENZA DI MISURAZIONE** | | Trimestrale | |
| **VALORE DI SOGLIA** | | Soglia minima: IQ016 ≥ 97,00% | |
| **PENALI** | | Il mancato raggiungimento del valore di soglia comporterà l'applicazione della penale pari allo 0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura, per ogni punto percentuale in diminuzione rispetto al valore soglia. | |

Relativamente all'indicatore di qualità "**Tempo di risoluzione**", è importante introdurre il concetto di "priorità" come elemento qualificante il problema. Di seguito la classificazione:

- **Priorità 1**: problema di tipo bloccante, per cui è impedito agli utenti l'utilizzo dei servizi ed alle eventuali componenti funzionali dei singoli servizi;
- **Priorità 2**: problema per cui è impedito agli utenti l'utilizzo di una funzione del servizio in alcune specifiche condizioni (ad esempio per alcuni dati di input);
- **Priorità 3**: richiesta di tipo informativo per cui risulta difficoltoso per gli utenti l'utilizzo di una funzione del servizio o sono necessarie ulteriori informazioni (o materiale documentale a supporto) o richiese relative a problematiche amministrative/contrattuali.

La seguente tabella indica i tempi massimi di risoluzione in funzione della priorità attribuita al problema.

| **Priorità del problema** | **T_max - Tempo massimo di risoluzione (ore lavorative)** |
|---|---|
| Priorità 1 | ≤ 4 ore |
| Priorità 2 | ≤ 8 ore |

| | |
|---|---|
| Priorità 3 | ≤ 12 ore |

Di seguito il dettaglio dell'indicatore:

| **ID** | **IQ017** | **PARAMETRO** | **Tempo di risoluzione** |
|---|---|---|---|
| **DESCRIZIONE** | | Tempestività nell'esecuzione delle attività necessarie alla risoluzione delle richieste ricevute tramite il servizio di Help Desk e relative ad anomalie e/o richiesta di informazioni. Sono comprese le richieste aperte in automatico dagli Strumenti di monitoraggio e controllo.<br>Il valore target è differenziato per il livello di priorità attribuito al problema ed è riportato nella tabella precedente; sulla base dei 3 distinti valori target, si differenzieranno 3 diversi indicatori di qualità: IQ017a, IQ017b e IQ017c, definiti sulla base della successiva formulazione. | |
| **FORMULA** | | IQ017a = $\frac{N_{richieste}\ (T_{risoluzione} \leq T_{Max_Priorità1})}{N_{richieste}}$ x 100<br>IQ017b = $\frac{N_{richieste}\ (T_{risoluzione} \leq T_{Max_Priorità2})}{N_{richieste}}$ x 100<br>IQ017c = $\frac{N_{richieste}\ (T_{risoluzione} \leq T_{Max_Priorità3})}{N_{richieste}}$ x 100<br>dove:<br>*T_risoluzione = Data_risol_ric – Data_aper_ric - T_pending*<br>e dove:<br>• *Data_aper_ric* = Data Ora (hh/mm/ss) della effettiva presa in carico;<br>• *Data_riso_ric* = Data Ora (hh/mm/ss) della risoluzione;<br>• *T_pending* = Tempo di pending complessivo;<br>• *N_richieste* = Numero totale di richieste. | |
| **FREQUENZA DI MISURAZIONE** | | Trimestrale | |
| **VALORE DI SOGLIA** | | Soglia minima:<br>IQ017a >= 99%<br>IQ017b >= 97%<br>IQ017c >= 95% | |
| **PENALI** | | Il mancato raggiungimento del valore di soglia comporterà l'applicazione della penale pari allo 1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni punto percentuale in diminuzione rispetto al valore soglia. | |

## *4 INDICATORI DI QUALITÁ PER IL SERVIZIO DI MIGRAZIONE*

| **ID** | **IQ018** | **PARAMETRO** | **Rispetto dei volumi previsti nel piano di migrazione** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore misura lo scostamento % tra i workload migrati e quelli previsti dal piano di migrazione concordato tra le parti in fase di progetto.<br>Per tener conto dei ritardi non dovuti al team di migrazione, andrà revisionato in modo coerente lo SLA target dell'anno e il target degli anni successivi. | |
| **FORMULA** | | $IQ018 = \frac{Numero_{workload_{previsti}} - Numero_workload_{migrati}}{Numero_workload_previsti} \times 100$ | |
| **FREQUENZA DI MISURAZIONE** | | Annuale | |
| **VALORE DI SOGLIA** | | Soglia minima:<br>IQ018 ≤ 10,00% per il primo anno<br>IQ018 ≤ 5,00% per gli anni successivi | |
| **PENALI** | | Il superamento del valore di soglia comporterà l'applicazione della penale pari allo 1,5% (unovirgolacinque per cento) dell'importo annuale, per ogni 10 punti percentuali in eccedenza rispetto al valore soglia. | |

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO B

## OFFERTA TECNICA

## Oggetto dell'Allegato

Il costituendo RTI TIM, in data 24 dicembre 2021, in sede di proposta di partenariato pubblico privato ai sensi dell'art. 183, comma 15, del D.lgs. n. 50/2016 s.m.i. ha presentato un Capitolato Tecnico con i relativi annessi, contenuto nell' Allegato A a questa Convenzione.

Il Dipartimento per la Trasformazione Digitale con Decreto n. 47/2021–PNRR, ha approvato il progetto di fattibilità e riconosciuto il costituendo RTI TIM come Promotore. Conseguentemente ha incluso il Capitolato Tecnico tra i documenti posti a base di Gara.

In fase di offerta e sulla base dell'art. 16 del Disciplinare di Gara, sia il costituendo RTI Fastweb sia il costituito RTI TIM hanno presentato la Relazione Tecnica Illustrativa contenente, ciascuna, le proprie proposte migliorative al fine di consentire l'attribuzione dei relativi punteggi, a seconda dei casi, tabellari oppure valutativi.

In particolare, in sede di Gara, le offerte tecniche sono state formulate dai concorrenti nei limiti della modificabilità del Capitolato tecnico posto a base di Gara, ovvero secondo le istruzioni dell'allegato 1 "Vademecum per il concorrente" al Disciplinare nonché della griglia di valutazione di cui al paragrafo 18.1 del disciplinare di Gara.

All'esito della Gara, l'offerta del RTI Fastweb ha conseguito un punteggio tecnico-economico complessivamente superiore a quello del RTI TIM. Pertanto, Difesa Servizi S.p.A., con nota del 22 giugno 2022, ha comunicato l'aggiudicazione al RTI Fastweb.

Tuttavia, come noto, ai sensi dell'art. 183, comma 15, del D.lgs. n. 50/2016 s.m.i., il Promotore, ai fini dell'aggiudicazione, può esercitare il diritto di prelazione se "*dichiara di impegnarsi ad adempiere alle obbligazioni contrattuali alle medesime condizioni offerte dall'aggiudicatario*". Tale dichiarazione è stata resa dal RTI TIM in data 7 luglio 2022; lo stesso RTI, pertanto, si è impegnato ad adempiere alle medesime condizioni contrattuali offerte dal RTI Fastweb. Conseguentemente, in data 11 luglio 2022, Difesa Servizi S.p.A. ha comunicato l'aggiudicazione al RTI TIM in qualità di Promotore prelazionario.

Prima dell'esercizio della prelazione, la centrale di committenza Difesa Servizi S.p.A., a seguito di specifico quesito del RTI TIM, con comunicazione n. 2538/2022 del 4 luglio 2022, ha chiarito che le "*soluzioni proprietarie, contenute nelle condizioni contrattuali offerte dall'aggiudicatario, potranno essere soddisfatte mediante soluzioni di carattere equivalente, nel rispetto dei principi di concorrenza e privativa*".

Vi sono, inoltre, prestazioni rispetto alle quali la Commissione giudicatrice ha assegnato all'offerta del RTI TIM un punteggio superiore o identico a quello dell'offerta del RTI Fastweb.

A tal proposito - fermo restando che l'offerta economicamente più vantaggiosa è quella dell'originario aggiudicatario RTI Fastweb, intendendosi con essa il livello minimo indefettibile di prestazioni che devono essere erogate a favore del Concedente in termini di *output* tecnico ed economico - il Concedente, in considerazione delle peculiarità tecniche e specialistiche del settore che investono l'organizzazione aziendale e il *know how* maturato che si traducono in elementi tipici e non replicabili dell'attività di ciascun operatore economico in un settore con alto grado di specializzazione, ha ritenuto opportuno determinare:

- in termini di maggiore garanzia dell'interesse pubblico, di fruire, a parità di prezzo e quindi di invarianza economica, di condizioni migliorative ulteriori rispetto al predetto minimo

indefettibile contrattuale;

- in termini di rispetto dei principi di concorrenza, della libertà di organizzazione aziendale e dei processi interni, che vengano erogate le predette prestazioni contrattuali secondo *input* tecnico-operativi ricompresi nelle capacità tecniche maturate dall'aggiudicatario esecutore tipiche della propria organizzazione interna e del proprio *know how* tecnologico.

In coerenza con quanto sopra il presente Allegato B - sulla base di quanto previsto dal Capitolato Tecnico con i relativi annessi e dalla Relazione tecnica del RTI Fastweb (Annesso 1), ivi inclusa la documentazione presentata a corredo della stessa - indica le soluzioni equivalenti e/o superiori che il Concessionario è autorizzato ad applicare in conformità ai principi di privativa, concorrenza, non discriminazione e tutela dell'interesse pubblico presenti nella Relazione Tecnica Illustrativa del RTI TIM (Annesso 2).

Rimangono in ogni caso integralmente ferme le più favorevoli condizioni della Relazione Tecnica Illustrativa del RTI Fastweb (Annesso 1).

## Esito dei lavori della Commissione giudicatrice

La Commissione giudicatrice della procedura di Gara, nominata il 4 giugno da Difesa Servizi con i verbali n. 2 del 24 maggio 2022 e n. 4 del 04 giugno 2022, ha provveduto ad assegnare i punteggi tecnici relativi alle proposte migliorative tabellari (verbale n. 2) e di carattere "valutativo" (verbale n. 4), secondo quanto previsto dal paragrafo 18 del Disciplinare di gara.

Le risultanze di tali valutazioni sono riassunte nelle seguenti tabelle:

| ID | Criterio | Punteggio Tabellare | RTI Fastweb | RTI TIM |
|---|---|---|---|---|
| 1 | Miglioramento dell'efficienza energetica dell'infrastruttura (PUE inferiore tra 1,45 e 1,30) | **4** | 4 | 4 |
| 2 | Riduzione dell'impatto ambientale (fonti rinnovabili tra 75% e 99%) | **6** | 6 | 6 |
| 3 | Comprovata competenza di gestione di informazioni personali (ISO/IEC 29100 e/o ISO/IEC 27701) | **2** | 2 | 2 |
| 4 | Comprovata competenza nella gestione di incidenti di sicurezza (ISO/IEC 27035-1 e/o 27035-2 | **2** | 2 | 2 |
| 5 | Incremento del numero di fornitori di servizi di public cloud (più di 3 CSP qualificati) | **1** | 1 | 1 |
| 6 | Miglioramento dell'offerta di servizi mediante utilizzo di tecnologia Open Source | **3** | 3 | 3 |
| 7, 8, 9 | Miglioramento degli indicatori di qualità | **5** | 5 | 5 |
| 10 | Parte migliorativa relativa alla riduzione dei tempi di disponibilità dell'infrastruttura (inferiore a 180 giorni) | **6** | 6 | 6 |
| 11 | Possesso, in capo al concorrente singolo o associato, della certificazione di responsabilità sociale ed etica SA 8000 o Equivalente | **2** | 2 | 2 |
| 12 | Impiego o assunzione di persone con disabilità in quota eccedente l'obbligo minimo di legge, nell'organico della società di progetto (NewCo) | **3** | 3 | 3 |
| 13 | Componente lavoro femminile superiore al 10% dell'organico della società di progetto (NewCo) | **3** | 3 | 3 |
| 14 | Componente lavoro giovanile (età inferiore a 36 anni) superiore al 5% dell'organico della società di progetto (NewCo) | **3** | 3 | 3 |
| | **TOTALE** | **40** | 40 | 40 |

**Verbale n. 2: Punteggi migliorativi tabellari**

| ID | Criterio | Punteggio Discrezionale | RTI Fastweb | RTI TIM |
|---|---|---|---|---|
| 15 | Modalità di verifica del rispetto delle norme ambientali | 3 | 3 | 3 |
| 16 | Miglioramenti sugli aspetti di ripartizione dei rischi | 3 | 3 | 2 |
| 17 | Miglioramenti sugli aspetti di governance | 4 | 3,36 | 4 |
| 18 | Miglioramenti sugli aspetti di aggiornamento prezzi | 3 | 3 | 2,68 |
| 19 | Miglioramento degli aspetti di cybersicurezza dell'infrastruttura. | 5 | 4,62 | 5 |
| 20 | Miglioramento delle modalità per la migrazione in cloud - Risorse e Tempistiche | 5 | 4,62 | 5 |
| 21 | Miglioramento delle modalità per la migrazione in cloud - Monitoraggio e gestione della migrazione | 3 | 2.74 | 3 |
| 22 | Mitigazione dei rischi connessi alla migrazione cloud | 4 | 2,55 | 4 |
| | TOTALE | 30 | 26,87 | 28,68 |

**Verbale n. 4: Punteggi migliorativi di carattere "valutativo"**

## Analisi dei punteggi "tabellari"

Dall'analisi della documentazione prodotta non emergono differenze rilevanti nelle offerte dei due RTI, come confermato dal medesimo punteggio tabellare che esse hanno ottenuto.

In merito al criterio ID 6 criterio relativo ai miglioramenti per l'introduzione di tecnologie Open Source, per il quale il Disciplinare ha richiesto espressamente di descrivere la componente tecnica e le tempistiche di disponibilità, il Concedente - in considerazione del punteggio attribuito dalla Commissione di gara - ha ritenuto opportuno prevedere che il riferimento per l'esecuzione del citato ID sia quello della Relazione Illustrativa del RTI TIM considerato che: a) la soluzione descritta dal RTI Fastweb contiene elementi di privativa (Fast Cloud Container); b) le implementazioni proposte (Open Stack-Open Shift, soluzioni Open Source di Oracle e Google per il RTI Fastweb e Open Source OKD e Mattermost per il RTI TIM) ancorché diverse fra di loro sono state ritenute equivalenti tanto da aver conseguito lo stesso punteggio.

Per tutti gli altri criteri (ID da 1 a 5 e da 7 a 14) dei punteggi tabellari rimane fermo il riferimento alla Relazione Tecnica illustrativa del RTI Fastweb (al netto delle descrizioni non esplicitamente richieste dal Disciplinare).

## Analisi dei punteggi "valutativi"

Per gli otto criteri di tipo valutativo, il RTI Fastweb ha proposto una soluzione migliore per gli ID 16 *"Miglioramento sugli aspetti di ripartizione dei rischi"* e ID 18 *"Miglioramento sugli aspetti di aggiornamento prezzi"*, in questi casi il RTI TIM eseguirà gli aspetti migliorativi descritti nella Relazione Illustrativa del RTI Fastweb.

Relativamente ai criteri descritti negli ID, 17 *"Miglioramenti sugli aspetti di governance"*, ID 19 *"Miglioramento degli aspetti di cybersicurezza dell'infrastruttura"*, ID 20 *"Miglioramento delle modalità per la migrazione in cloud - Risorse e tempistiche"*, ID 21 *"Miglioramento delle modalità per la migrazione in cloud - Monitoraggio e gestione della migrazione"* e ID 22 *"Mitigazione dei rischi connessi alla migrazione cloud"*, il Concessionario eseguirà le soluzioni adottate nella propria offerta a maggiore soddisfazione dell'interesse pubblico, avendo in questi casi conseguito un punteggio superiore a quello del RTI Fastweb. In questi ID, pertanto, il riferimento è la Relazione Tecnica illustrativa del RTI TIM.

Per l'ID 15 *"Modalità di verifica del rispetto delle norme ambientali"*, in considerazione del citato criterio di equivalenza funzionale delle offerte, determinato oltre che sulla base dei principi di privativa e concorrenza anche sulla base delle peculiari caratteristiche tecnico-operative proprie di ogni operatore

economico in ambiti specialistici quale quello in argomento, il Concessionario eseguirà le soluzioni indicate nella propria offerta relativamente a tale criterio. Tale parametro aveva come descrizione del criterio "*Efficacia delle modalità di verifica proposte dal Concessionario, messe a disposizione del concedente, per il rispetto delle seguenti norme e standard europei in materia ambientale (Do no significant harm): - ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD(2020) 55 final); - Indipendenza energetica e fonti rinnovabili; - Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE); - Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva; - Le procedure di approvvigionamento includeranno la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali; - Al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della direttiva 2012/19/UE*". Trattandosi, pertanto, di certificazioni ISO o similari e del rispetto di normative europee è evidente che le stesse attengono al processo produttivo delle singole imprese, sulla base anche dei Data Center coinvolti, confermando quindi il criterio di equivalenza. L'adozione di tale criterio di equivalenza è anche giustificata dalla privativa derivante dai Data Center, intesi come costruzione, localizzazione, e tutte le altre loro caratteristiche identitarie, che erano già state oggetto di una specifica previsione nel Disciplinare (*rif.* Vademecum per il concorrente).

Tenendo conto dell'adozione delle soluzioni equivalenti e/o superiori di cui al presente documento, resta confermata la sostenibilità del piano economico-finanziario del Concessionario.

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ANNESSI
# DELL'ALLEGATO B

## Oggetto degli Annessi all'allegato B

Gli annessi all'allegato B sono costituiti dai seguenti documenti:

- Annesso 1: Relazione tecnica illustrativa dell'RTI Fastweb;
- Annesso 2: Relazione tecnica illustrativa dell'RTI TIM;

Procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico-privato, della realizzazione e gestione del Polo Strategico Nazionale
CIG: 9066973ECE
CUP: J51B21005710007

# RELAZIONE TECNICA ILLUSTRATIVA

# INDICE GENERALE


INDICE GENERALE ..... 2

INDICE DELLE TABELLE E DELLE FIGURE ..... 4

DEFINIZIONI ..... 6

PREMESSA ..... 7

1 DESCRIZIONE DEI CRITERI DI VALUTAZIONE ..... 8

1.1 id criterio:1 – tabellare - miglioramento del PUE misurato su base annuale per ciascun anno e per ciascun Data Center a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 1,5 ..... 8

1.2 id criterio:2 – tabellare - miglioramento della % di approvvigionamento elettrico da fonti rinnovabili anche ai fini dell'indipendenza energetica per il relativo approvvigionamento misurato per ciascun Data Center su base annuale per ciascun anno a partire dal secondo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 50% ..... 9

1.3 id criterio:3 – tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di informazioni personali, quali certificazioni della famiglia ISO/IEC 29100 oppure ISO/IEC 2770110

1.4 id criterio:4 – tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di incidenti di sicurezza, quali la ISO 27035 ..... 11

1.5 id criterio:5 – tabellare – incremento del numero di fornitori di servizi di *Public Cloud* (CSP qualificati) rispetto al valore base della proposta pari a 3 con i quali il concorrente si impegna a far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: *Public Cloud* PSN *Managed*, Secure *Public Cloud*, *Hybrid Cloud* on PSN *Site* ..... 12

1.6 id criterio:6 – tabellare - Miglioramento dell'offerta di servizi *cloud* mediante utilizzo di tecnologia *Open Source*. Per tali servizi, l'offerta tecnica deve prevedere la descrizione della componente tecnica e la descrizione delle tempistiche di disponibilità di tali servizi che saranno inseriti in sede di aggiornamento del listino prezzi, comunque non oltre i 2 anni dalla sottoscrizione della Convenzione ..... 13

1.7 id criterio:7 –tabellare - Miglioramento del valore soglia dell'indicatore di qualità IQ04 pari a numero 5 rilievi ..... 24

1.8 id criterio:8 – tabellare - Miglioramento dei seguenti valori: RTO atteso dell'indicatore di qualità IQ11 pari a 30 minuti, RPO *target* dell'indicatore di qualità IQ12 pari a 1 minuto, RTO su diversa *Region* atteso dell'indicatore di qualità IQ13 pari a 4 ore, RPO su diversa *Region target* dell'indicatore di qualità IQ14 pari a 30 minuti ..... 25

1.9 id criterio:9 – tabellare - Miglioramento dei valori soglia dell'indicatore di qualità IQ017 con riferimento ai tempi massimi di risoluzione in ore (Priorità 1 <= 4 ore; Priorità 2 <= 8 ore; Priorità 3 <=12 ore) ..... 31

1.10 id criterio:10 – tabellare – Riduzione sul periodo minimo di disponibilità dell'infrastruttura di 180 giorni. Il cronoprogramma dovrà evidenziare tutti gli step relativi alla disponibilità dell'infrastruttura evidenziando le proposte che presentino la maggior celerità realizzativa. ..... 43

1.11 id criterio:11 – tabellare - Possesso, in capo al concorrente singolo o associato, della certificazione di responsabilità sociale ed etica SA 8000 o equivalente ..... 52

1.12 id criterio:12 – tabellare - Impiego o assunzione di persone con disabilità in quota eccedente l'obbligo minimo di legge, nell'organico della società di progetto (NewCo) ..... 53

1.13 id criterio:13 – tabellare - Componente lavoro femminile superiore al 10% dell'organico della società di progetto (NewCo) ..... 53

1.14 id criterio:14 – tabellare - Componente lavoro giovanile (età inferiore a 36 anni) superiore al 5% dell'organico della società di progetto (NewCo) ..... 54

1.15 id criterio:15 – valutativo - Efficacia delle modalità di verifica proposte dal Concessionario, messe a disposizione del concedente, per il rispetto delle seguenti norme e standard europei in materia ambientale (*Do no significant harm*):..... 55

1.16 id criterio:16 – valutativo - Miglioramenti, a favore del Concedente, della matrice di ripartizione del rischio. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. ..... 71

1.17 id criterio:17 – valutativo - Miglioramenti del modello di governance utili a consentire un maggior coinvolgimento del Concedente anche nell'ottica di garantire ulteriormente la vigilanza e il monitoraggio pubblico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. ..... 82

1.18 id criterio:18 – valutativo - Miglioramenti, a favore del Concedente, della *compliance* nell'aggiornamento dei costi e prezzi dell'infrastruttura anche da un punto di vista del *refresh* tecnologico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. ..... 93

1.19 id criterio:19 – valutativo - Miglioramenti sulla proposta progettuale per quanto riguarda gli aspetti relativi all'integrazione del PSN con l'Architettura Nazionale Cyber, con particolare riguardo alle modalità ed ai processi per l'integrazione con lo CSIRT Italia (fino a 1 punto), alla messa a disposizione di funzionalità per l'interazione con gli ISAC (fino a 1,5 punti), messa a disposizione di funzionalità per scambio di informazioni A2A tra il SOC e lo CSIRT Italia (fino a 2,5 punti) ..... 97

1.20 id criterio:20 – valutativo - Completezza, accuratezza e verificabilità del metodo che il concorrente si impegna ad adottare per la definizione del dimensionamento delle risorse (giorni/uomo e relativo team mix per tipologia di strategia di migrazione) e delle tempistiche per la realizzazione di ciascuna fase di ciascun progetto di migrazione per gli scenari 1, 2 e 3 e per i casi di "breve termine" e "medio e lungo termine" ..... 117

1.21 id criterio:21 – valutativo - Miglioramenti del modello organizzativo, delle metodologie e degli strumenti che il concorrente si impegna ad adottare per il monitoraggio ed il controllo della migrazione al fine del rispetto delle tempistiche previste. ..... 128

1.22 id criterio:22 – valutativo - Miglioramenti della strategia di mitigazione dei rischi connessi alla migrazione dei servizi delle amministrazioni (disponibilità, integrità e performance) ..... 141

# INDICE DELLE TABELLE E DELLE FIGURE

*Indice delle tabelle:*


Tabella 1: Categorizzazione del livello di impatto di un incident ..... 38
Tabella 2: Definizione priorità degli Incident ..... 39
Tabella 3: Livelli di servizio offerti dall'Offerente ..... 39
Tabella 4: CMDB – Asset discovery ..... 42
Tabella 5: Milestone del Cronoprogramma ..... 46
Tabella 6: Descrizione attività del Gantt ..... 47
Tabella 7: A comprehensive examination of the metric - White Paper #49, The Green Grid ..... 65
Tabella 8: Classificazione dei risultati PUE secondo la Green Grid Association ..... 66
Tabella 9: Nuova Matrice dei Rischi proposta dall'Offerente - migliorie in rosso ..... 75
Tabella 10: Esempio di report di monitoraggio SLA ..... 92
Tabella 11: Aree PNRR supportate dalle iniziative della NewCo ..... 101
Tabella 12: Scenari di complessità della migrazione ..... 124
Tabella 13: Team mix per scenari di migrazione ..... 128
Tabella 14: Tipologie di meeting ..... 130
Tabella 15: Classi delle CRQ ..... 136
Tabella 16: Rischi di migrazione ed azioni di mitigazione ..... 141
Tabella 17: Misure di Sicurezza per strategia di migrazione ..... 142


*Indice delle Figure:*


Figura 1: Mappatura CSP ..... 13
Figura 2: Modello Open Source ..... 15
Figura 3: Combinazione OpenShift e OpenStack ..... 17
Figura 4: I servizi principali di OpenStack ..... 18
Figura 5: Openshift KMS ..... 19
Figura 6: Openshift nella architettura Hybrid Cloud on PSN Site ..... 21
Figura 7: FASTcloud container ..... 23
Figura 8: FASTcloud container deployment scenarios ..... 24
Figura 9: Strategia di sito ..... 26
Figura 10: Region ad alta affidabilità ..... 27
Figura 11: Repliche sincrone e asincrone tra Availability Zone ..... 28
Figura 12: Schema di interconnessione fra i DC ..... 29
Figura 13: RPO e RTO - Automation and Orchestration ..... 31
Figura 14: Sistema di monitoraggio degli eventi infrastrutturali ..... 33
Figura 15: Fasi di Incident Management ..... 35
Figura 16: Fasi del Problem Management ..... 36
Figura 17: Interazione tra Incident e Problem Management ..... 37
Figura 18: Risultati della soluzione di Automation ..... 40
Figura 19: Soluzione di Automation (Incident, Problem, Change Management) ..... 41
Figura 20: Cronoprogramma ..... 45
Figura 21: Gantt ..... 47
Figura 22: Certificati di annullamento Fastweb Garanzie d'origine (2020) ..... 56
Figura 22: Certificato di garanzia rilasciato da Duferco Energia ad Aruba S.p.A. ..... 57
Figura 24: Centrali idroelettriche acquistate da Aruba in Italia ..... 57

Figura 24: Pannelli fotovoltaici installati sui DC ..... 57
Figura 25: Impianto geotermico per i sistemi di raffreddamento degli apparati ..... 58
Figura 26: Funzionamento del Dynamic Free Cooling ..... 58
Figura 28: Dashboard di costi cloud per servizio ed elemento infrastrutturale ..... 89
Figura 29: Report di performance dell'infrastruttura ..... 91
Figura 30: Vista settimanale per diversa tipologia di ticket ..... 92
Figura 31: Trend annuale per diversa tipologia di ticket ..... 93
Figura 32: Ruolo strategico della Cybersecurity - Fonte: AgiD Italia digitale 2026 ..... 101
Figura 33: Scambio informazioni per la mitigazione del rischio ..... 104
Figura 34: Caratteristiche ISAC ..... 104
Figura 35: Flussi informativi degli indicatori di compromissione ..... 106
Figura 36: Analisi eventi notevoli ..... 106
Figura 37: Processo di elaborazione dell'architettura HPC ..... 108
Figura 38: Strutture che partecipano all'erogazione dei servizi di sicurezza ..... 112
Figura 39: Categorie servizi erogati da un CERT ..... 113
Figura 40: Flusso logico di valutazione dell'applicativo ..... 119
Figura 41: Flusso logico di valutazione infrastrutturale ..... 121
Figura 42: Scenari di migrazione: modello delle 6R ..... 121
Figura 43: Caso di consolidamento ..... 122
Figura 44: Casi di applicativo virtualizzabile ..... 122
Figura 45: Casi di applicativo cloud Ready e cloud Native ..... 123
Figura 46: Caso SaaS ..... 123
Figura 47: Scenari di migrazione per la PA ..... 124
Figura 48: Piano di migrazione (esemplificativo) ..... 125
Figura 49: Modello Operativo ad alto livello ..... 129
Figura 50: Dashboard di progetto (illustrativa) ..... 131
Figura 51: Modello Operativo ad alto livello: funzione di Service Management ..... 131
Figura 52: Dashboard dei KPI del tool di Clash management ..... 137
Figura 53: Dashboard di rilevazione dei conflitti ..... 138
Figura 54: Vista dello strumento HPE Right Mix Advisor ..... 139
Figura 55: Funzionamento dello strumento HCX ..... 140

# DEFINIZIONI

Nel seguito del documento valgono le seguenti **definizioni**, declinate sia al singolare che al plurale:

a. **Addendum**: *Addendum* alla bozza di convenzione (Allegato 10 al Disciplinare);
b. **AgID:** indica l'Agenzia per l'Italia Digitale, istituita ai sensi dell'articolo 19 del D.L. del 22 giugno 2012, n. 83, convertito in legge, con modificazioni, dall'art. 1 della legge 7 agosto 2012, n. 134 e ss.mm.ii., preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana;
c. **AI**: *Artificial Intelligence*
d. **Amministrazione utente o PA utente**: amministrazioni utenti del PSN;
e. **Bando o Bando di Gara**: stessa definizione presente nella Bozza di Convenzione;
*f.* **BC**: *business continuity;*
g. **BdC o Bozza di Convenzione**: la bozza di convenzione, (Allegato 3 - *sub* 6 al Disciplinare), comprensiva dei suoi allegati;
h. **Comitato**: il Comitato di Controllo, a norma dell'art. 12 della BdC;
i. **Concedente:** indica il Ministero per l'Innovazione Tecnologica e la Transizione Digitale;
j. **Concessionario:** indica il soggetto affidatario della concessione per la realizzazione e gestione del PSN, ossia la NewCo;
k. **CRQ**: *Change Request*;
l. **CSP:** *Cloud Service Provider*;
m. **Data Center o DC**: stessa definizione presente nella Bozza di Convenzione;
n. **Disciplinare**: indica il documento "Disciplinare di gara PSN_ (1)_signed", dal titolo "*Disciplinare di gara europea, a procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico-privato, della realizzazione e gestione del polo strategico nazionale*";
o. **Documentazione di Gara**: stessa definizione della Bozza di Convenzione;
p. **Documento contenente la descrizione dei servizi o Capitolato Servizi:** indica l'Allegato 3 - *sub* 2 al Disciplinare;
q. **DR:** *Disaster Recovery;*
r. **Enti preposti:** indica il Concedente, l'ANC, l'AgID e gli altri enti titolari di funzioni di controllo e monitoraggio sul PSN;
s. **Matrice**: la matrice dei rischi (allegato *sub* G alla BdC);
t. **MITD**: indica il Ministero per l'innovazione tecnologica e la transizione digitale;
u. **NewCo**: la società di progetto concessionaria del PSN;
v. **Offerente o RTI**: il costituendo RTI concorrente composto da Fastweb S.p.a. ed aruba S.p.a.;
w. **Offerta o Offerta Fastweb-Aruba**: l'offerta del costituendo RTI tra Fastweb S.p.a. ed aruba S.p.a.;
x. **Progetto di Fattibilità**: indica il documento Allegato 3 - *sub* 1 al Disciplinare;
y. **PSN**: Polo Strategico Nazionale;
z. **R&D**: ricerca e sviluppo;
aa. **Relazione**: la presente relazione illustrativa tecnica dell'Offerta;
bb. **SDN**: *Software Defined Networking*;
*cc.* **SOAR**: *Security Orchestration, Automation and Response*.

# PREMESSA

La presente Relazione fa parte dell'Offerta, predisposta dall'Offerente, in risposta alla "*Procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico-privato, della realizzazione e gestione del Polo Strategico Nazionale*" del 28 gennaio 2022.

Con l'Offerta, l'Offerente, costituendo RTI tra Fastweb ed aruba, accetta *in toto* i contenuti della proposta a base di gara, e tutta la documentazione ad essa afferente, ivi inclusa la Bozza di Convenzione, comprensiva dei suoi allegati, e relativo Addendum.

Con la presente Relazione, l'Offerente intende illustrare i contenuti e le caratteristiche tecniche che caratterizzano l'Offerta, che costituiscono migliorie o specificazioni rispetto agli elementi posti a base di gara. La Relazione riporta in maniera progressiva, per ogni criterio indicato nella tabella n. 5 del Disciplinare, le migliorie e soluzioni offerte al fine di consentire l'attribuzione del relativo punteggio (tabellare ovvero valutativo).

Inoltre, ove dovessero sorgere dubbi interpretativi tra l'intera documentazione costituente la c.d."*lex specialis*" di gara e l'Offerta, l'Offerente precisa che si atterrà, comunque, alle prescrizioni della *lex specialis*.

# 1 DESCRIZIONE DEI CRITERI DI VALUTAZIONE

## 1.1 ID CRITERIO:1 – TABELLARE - MIGLIORAMENTO DEL PUE MISURATO SU BASE ANNUALE PER CIASCUN ANNO E PER CIASCUN DATA CENTER A PARTIRE DAL TERZO ANNO DALLA STIPULA DEL CONTRATTO E DA MANTENERE PER TUTTI GLI ANNI SUCCESSIVI FINO ALLA SCADENZA DEL CONTRATTO RISPETTO AL VALORE BASE PARI A 1,5

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 1 | Tabellare | Ambientale | Miglioramento dell'efficienza energetica dell'infrastruttura | Miglioramento del PUE misurato su base annuale per ciascun anno e per ciascun Data Center a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 1,5 | 1 punto | per PUE pari a 1,45 | 4 |
| | | | | | 2 punti | per PUE pari a 1,4 | |
| | | | | | 3 punti | per PUE pari a 1,35 | |
| | | | | | 4 punti | PUE pari o inferiore a 1,3 | |

Le società che costituiscono l'Offerente sono molto attive sui temi di protezione ambientale, come anche evidente da quanto riportato nella risposta al criterio numero 15, vedi capitolo 1.15. Il PUE è uno degli indicatori che sono costantemente monitorati con l'obiettivo di migliorarne, nel tempo, il valore raggiunto e contribuire in modo concreto al rispetto dell'ambiente. Relativamente ai DC che saranno impiegati per il PSN, alcuni di questi offrono già oggi un PUE "*best in class*", con valori inferiori a 1,3 (unovirgolatre).

In merito ai DC che oggi non raggiungono tale livello di PUE, invece, saranno presi gli opportuni accorgimenti per migliorarne la *performance*. In particolare, si evidenzia che il PUE misurato annuo dipende da fattori sia statici che variabili:

- tra i fattori statici si citano l'efficienza degli impianti elettrici (UPS, dimensionamenti) e meccanici (*chiller*, *free-cooling*, CRAH, CRAC);
- tra i fattori variabili si citano la percentuale di carico IT rispetto al carico di progetto ottimale, le temperature medie esterne annue e la conduzione e manutenzione (in particolare affinamento dei settaggi, ottimizzazione aeraulica, corretta manutenzione di impianti elettrici e meccanici).

Pertanto, gli accorgimenti che l'Offerente si impegna a garantire per l'ottimizzazione del PUE consistono nel continuo e proattivo monitoraggio preventivo ai fini di tenere sempre *standard* di conduzione e manutenzione molto elevati, nell'ottimizzazione del carico IT all'interno del DC ed a continue attività di R&D per il miglioramento dell'efficienza energetica dei singoli impianti.

Sulla base di quanto sopra, l'Offerente si **impegna a garantire i seguenti valori di PUE medio**, misurato su base annuale a partire dal terzo anno dalla stipula del contratto, come richiesto dal criterio espresso nel Bando di gara, ed a mantenerli anche per gli anni successivi:

| Data Center | Valore PUE garantito |
|---|---|
| DC1- *Region* Nord | <1,3 |
| DC2 - *Region* Nord | <1,3 |
| DC3 - *Region* Centro-Sud | <1,3 |
| DC4 - *Region* Centro-Sud | <1,3 |

Questo impegno rappresenta un **chiaro miglioramento rispetto al valore base riportato nella documentazione di gara**, pari ad un PUE di 1,5 (uno virgola cinque), come descritto nella seguente tabella di sintesi:

Miglioramento del PUE

| Punteggio indirizzato dall'Offerente = 4 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore PUE Base:<br><br>1,5<br><br>Misurato su base annuale per ciascun anno e per ciascun *Data Center* a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto | Valore PUE dell'Offerente:<br><br>DC1: <1,30<br>DC2: <1,30<br>DC3: <1,30<br>DC4: <1,30<br><br>Misurato su base annuale per ciascun anno e per ciascun *Data Center* a partire dal terzo anno dalla stipula del contratto e mantenuto per tutti gli anni successivi fino alla scadenza del contratto |

## 1.2 ID CRITERIO:2 – TABELLARE - MIGLIORAMENTO DELLA % DI APPROVVIGIONAMENTO ELETTRICO DA FONTI RINNOVABILI ANCHE AI FINI DELL'INDIPENDENZA ENERGETICA PER IL RELATIVO APPROVVIGIONAMENTO MISURATO PER CIASCUN DATA CENTER SU BASE ANNUALE PER CIASCUN ANNO A PARTIRE DAL SECONDO ANNO DALLA STIPULA DEL CONTRATTO E DA MANTENERE PER TUTTI GLI ANNI SUCCESSIVI FINO ALLA SCADENZA DEL CONTRATTO RISPETTO AL VALORE BASE PARI A 50%

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| **2** | Tabellare | Ambientale | Riduzione dell'impatto ambientale | Miglioramento della % di approvvigionamento elettrico da fonti rinnovabili anche ai fini dell'indipendenza energetica per il relativo approvvigionamento misurato per ciascun Data Center su base annuale per ciascun anno a partire dal secondo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 50% | 1,5 punti | per valori dal 51% fino al 75% | **6** |
| | | | | | 3 punti | per valori dal 76% al 90% | |
| | | | | | 4,5 punti | per valori dal 91 al 99% | |
| | | | | | 6 punti | per valori superiori al 99% | |

Le società, parti dell'Offerente, sono attive su diversi fronti per la riduzione dell'impatto ambientale. In questo contesto, hanno attivato diversi contratti per la fornitura di energia elettrica da fonti rinnovabili.
In particolare, **i DC, oggi individuati per il PSN, sono già alimentati al 100% da energia elettrica proveniente da fonti rinnovabili e così sarà anche per il futuro**. Questa caratteristica sarà disponibile, a partire dal secondo anno, e mantenuta per tutta la durata della Concessione per tutti i DC.

Il **miglioramento** proposto è **evidente** rispetto al valore base, pari al 50%, come descritto nella tabella seguente:

% approvvigionamento elettrico da fonti rinnovabili

| Punteggio indirizzato dall'Offerente = 6 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 50%<br><br>Misurato su base annuale per ciascun anno a partire dal secondo anno e da mantenere per tutti gli anni successivi fino alla scadenza del contratto | Valore dell'Offerente: 100%<br><br>Misurato su base annuale per ciascun anno a partire dal secondo anno e mantenuto per tutti gli anni successivi fino alla scadenza del contratto |

## 1.3 ID CRITERIO:3 – TABELLARE - TITOLARITÀ DI CERTIFICAZIONI DI SICUREZZA IN MATERIA DI GESTIONE DI INFORMAZIONI PERSONALI, QUALI CERTIFICAZIONI DELLA FAMIGLIA ISO/IEC 29100 OPPURE ISO/IEC 27701

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 3 | Tabellare | Cybersecurity | Comprovata competenza di gestione di informazioni personali. | Titolarità di certificazioni di sicurezza in materia di gestione di informazioni personali, quali certificazioni della famiglia ISO/IEC 29100 oppure ISO/IEC 27701. | 1 punto | ISO/IEC 29100 o ISO/IEC 27701 | 2 |
| | | | | | 2 punti | ISO/IEC 29100 e ISO/IEC 27701 | |

Fastweb, in qualità di mandataria del costituendo RTI, è titolare di certificazioni di entrambe le famiglie specificate nel criterio tabellare. Si allegano i certificati relativi agli *standard* ISO27701 ed al personale in possesso della ISO 29100 nei seguenti file.

<u>ISO 27701:</u>

- Relazione tecnica - Allegato 3.1 - FASTWEB SPA - ISOIEC 27701

<u>ISO 29100:</u>

- Relazione tecnica - Allegato 3.2 - ISO 29100 - Certificato Adolfo Pandolfi_(31gen2022).pdf
- Relazione tecnica - Allegato 3.3 - ISO 29100 - Certificato Esmeralda Konika_(31gen2022).pdf
- Relazione tecnica - Allegato 3.4 - ISO 29100 - Certificato Jessica Ghietti_(31gen2022).pdf

- Relazione tecnica - Allegato 3.5 - ISO 29100 - Certificato William Perfetto_(31gen2022).pdf

Titolarità certificazioni di sicurezza in materia di gestione di informazioni personali

| Punteggio indirizzato dall'Offerente = 2 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 0<br><br>Certificazioni della famiglia ISO/IEC 29100 oppure ISO/IEC 27701 non previste nella documentazione di gara. | Valore dell'Offerente: 2<br><br>Titolarità di entrambe le certificazioni della famiglia ISO/IEC 29100 e ISO/IEC 27701 |

## 1.4 ID CRITERIO:4 – TABELLARE - TITOLARITÀ DI CERTIFICAZIONI DI SICUREZZA IN MATERIA DI GESTIONE DI INCIDENTI DI SICUREZZA, QUALI LA ISO 27035.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 4 | Tabellare | Cybersecurity | Comprovata competenza nella gestione di incidenti di sicurezza. | Titolarità di certificazioni di sicurezza in materia di gestione di incidenti di sicurezza, quali la ISO 27035 | 1 punto | ISO/IEC 27035-1 | 2 |
| | | | | | 2 punti | ISO/IEC 27035-1 e 27035-2 | |

Fastweb, in qualità di mandataria del costituendo RTI, dispone di entrambe le certificazioni riportate nel criterio 4 (ISO27035-1 e ISO 27035 – 2) e della ISO27035-3. Si allegano i certificati nel seguente allegato alla Relazione:

- Relazione tecnica - Allegato 4.1 - FASTWEB SPA - ISOIEC 27035

Titolarità certificazioni di sicurezza in materia di gestione di incidenti di sicurezza

| Punteggio indirizzato dall'Offerente = 2 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 0<br><br>Certificazioni di sicurezza in materia di gestione di incidenti di sicurezza non previste nel bando di gara. | Valore dell'Offerente: 2<br><br>L'Offerente dispone sia della certificazione ISO/IEC 27035-1, che della certificazione 27035-2 |

## 1.5 ID CRITERIO:5 – TABELLARE – INCREMENTO DEL NUMERO DI FORNITORI DI SERVIZI DI *PUBLIC CLOUD* (CSP QUALIFICATI) RISPETTO AL VALORE BASE DELLA PROPOSTA PARI A 3 CON I QUALI IL CONCORRENTE SI IMPEGNA A FAR STIPULARE ACCORDI ALLA NEWCO PER L'OFFERTA DEI SERVIZI IN TUTTI I SEGUENTI AMBITI: *PUBLIC CLOUD* PSN *MANAGED*, SECURE *PUBLIC CLOUD*, *HYBRID CLOUD* ON PSN *SITE*

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|
| **5** | Tabellare | Tecnologie *Cloud* | Incremento del numero di fornitori di servizi di *Public Cloud* (CSP qualificati) | Incremento del numero di fornitori di servizi di *Public Cloud* (CSP qualifcati) rispetto al valore base della proposta pari a 3 con i quali il concorrente si impegna a far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: *Public Cloud* PSN *Managed*, *Secure Public Cloud*, *Hybrid Cloud on* PSN *Site* | **Più di 3 CSP qualificati** | **1** |

Il numero di CSP qualificati previsti nell'Offerta **è pari a 4,** come meglio descritto nel seguito della Relazione e nell'Annesso. I CSP utilizzati nell'Offerta per i servizi PSN sono:

- Amazon Web Services (AWS);
- Google Cloud;
- Microsoft;
- Oracle.

Con questi CSP, l'Offerente si impegna a far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: *Public Cloud* PSN *Managed*, *Secure Public Cloud*, *Hybrid Cloud on* PSN *Site*.

Numero di fornitori di servizi di *Public Cloud* (CSP qualificati)

| Punteggio indirizzato dall'Offerente = 1 punto | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 3 CSP | Valore dell'Offerente: 4 CSP |

### 1.5.1 Mappa dei CSP supportati

Per completezza, si riporta di seguito uno schema di sintesi, simile a quello riportato nel Progetto di fattibilità, capitolo 2.9, con la mappatura dei fornitori dei servizi *Public Cloud* supportati dall'Offerta. Per maggiori dettagli si faccia riferimento all'Annesso, capitolo 2.

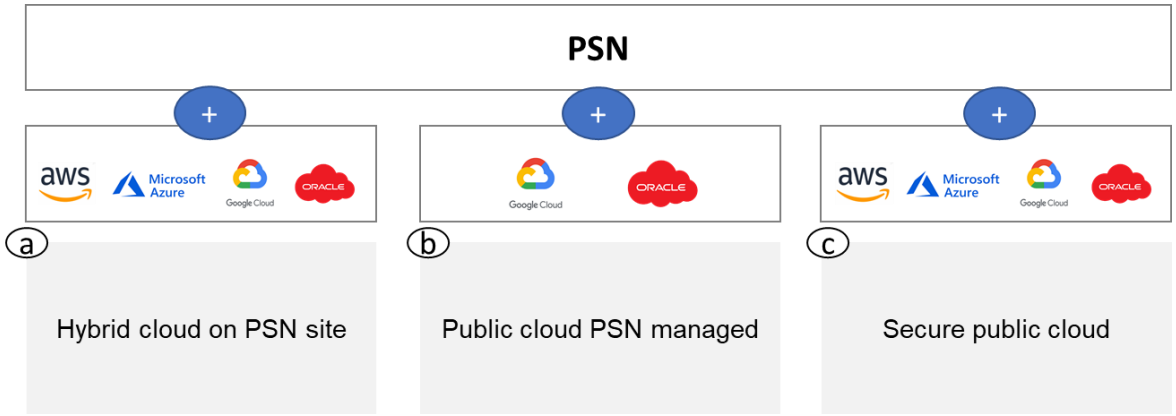



*Figura 1: Mappatura CSP*

## 1.6 ID CRITERIO:6 – TABELLARE - MIGLIORAMENTO DELL'OFFERTA DI SERVIZI *CLOUD* MEDIANTE UTILIZZO DI TECNOLOGIA *OPEN SOURCE*. PER TALI SERVIZI, L'OFFERTA TECNICA DEVE PREVEDERE LA DESCRIZIONE DELLA COMPONENTE TECNICA E LA DESCRIZIONE DELLE TEMPISTICHE DI DISPONIBILITÀ DI TALI SERVIZI CHE SARANNO INSERITI IN SEDE DI AGGIORNAMENTO DEL LISTINO PREZZI, COMUNQUE NON OLTRE I 2 ANNI DALLA SOTTOSCRIZIONE DELLA CONVENZIONE

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| **6** | Tabellare | Tecnologie *Cloud* | Miglioramento dell'offerta di servizi mediante utilizzo di tecnologia *Open Source* | Miglioramento dell'offerta di servizi *cloud* mediante utilizzo di tecnologia *Open Source*. Per tali servizi, l'offerta tecnica deve prevedere la descrizione della componente tecnica e la descrizione delle tempistiche di disponibilità di tali servizi che saranno inseriti in sede di aggiornamento del listino prezzi, comunque non oltre i 2 anni dalla | **1 punto** | per incremento offerta di:<br>- (i) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito dei servizi *Private Cloud* | **3** |
| | | | | | **2 punti** | per incremento offerta di:<br>- (i) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito dei servizi *Private Cloud*<br>- (ii) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito dei servizi *Public Cloud* PSN *Managed* | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | sottoscrizione della Convenzione | **3 punti** | per incremento offerta di:<br>- (i) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito dei servizi *Private Cloud*<br>- (ii) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito dei servizi *Public Cloud* PSN *Managed*<br>- (iii) almeno 1 servizio *cloud* basato su tecnologia *Open Source* nell'ambito di *Secure Public Cloud* e *Hybrid Cloud on* PSN *Site* | |

In merito al criterio 6, l'Offerente propone diverse migliorie - come sintetizzato nella tabella seguente - descritte con maggior dettaglio nei paragrafi successivi. In particolare, l'Offerente ha selezionato **le seguenti tecnologie *Open Source* per tutti e tre gli ambiti** previsti dal criterio di valutazione:

1. OpenStack-OpenShift;
2. *Open Source* su architettura Oracle Cloud;
3. *Open Source* su architettura Google Cloud;
4. FASTcloud Container.

Le tempistiche di disponibilità, descritte nel dettaglio nella sezione 1.6.1 del presente criterio, sono coerenti con quanto previsto nella documentazione di gara (non oltre i 2 anni dalla sottoscrizione della Convenzione).

Miglioramento dell'offerta mediante l'utilizzo di tecnologia *Open Source*

| Punteggio indirizzato dall'Offerente = 3 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 0 servizi *Open Source*<br><br>Nessun servizio *cloud* basato su tecnologia *Open Source* è strettamente richiesto nel bando di gara. | Valore dell'Offerente: più di 3 servizi *Open Source, di cui almeno 1 per ogni ambito previsto dal criterio*<br><br>Utilizzo di tecnologie *Open Source* per tutti e tre gli ambiti previsti dal criterio in oggetto (*Private, Public Managed* e *Secure/Hybrid*) |

### 1.6.1 Soluzioni *Open Source* e tempistiche proposte

Il caposaldo dell'approccio *Open Source* è lo sviluppo di codice *software* tramite un modello decentralizzato e collaborativo, che si fonda sulla "*peer review*", ovvero le revisioni condotte da colleghi e professionisti, e sul lavoro della comunità. Il *software* sviluppato dalla comunità viene rilasciato senza essere vincolo di proprietà intellettuale, lasciando la completa disponibilità del codice sorgente.
Per il PSN, che si pone l'obiettivo di garantire la sovranità sulle infrastrutture applicative e preservare l'autonomia tecnologica del Paese, l'utilizzo pervasivo di tecnologie *Open Source* è un fattore fortemente abilitante; avendo a disposizione il codice sorgente del *software* è

possibile effettuare un *audit* di sicurezza continuativo sulle applicazioni ed è garantita completa autonomia da un qualsiasi vincolo di fornitura in qualunque scenario possibile.

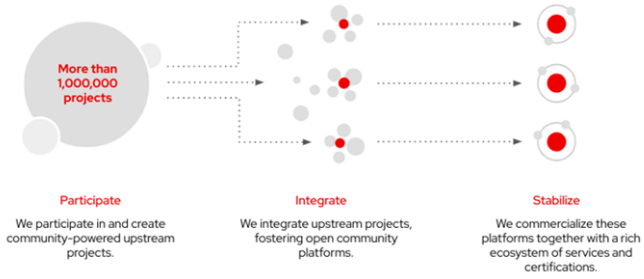



*Figura 2: Modello Open Source*

Per queste ragioni l'Offerente farà largo uso di tecnologie *Open Source*, adottandole secondo due direttrici:

- affiancando, su tutto il suo portafoglio servizi, le soluzioni tecnologiche *Open Source* alle soluzioni basate su *software* proprietario;
- selezionando, anche nell'ambito delle soluzioni sviluppate con i *partner* operatori del *cloud*, componenti e servizi che si basano su tecnologia *Open Source*.

Le tempistiche con cui tali tecnologie saranno rese disponibili nell'ambito del PSN sono specificate di seguito:

- OpenStack, OpenShift ed a*dvanced Cluster Manager* (RHACM) sono soluzioni già disponibili sul mercato. La loro usabilità su infrastrutture PSN seguirà il *provisioning* delle specifiche soluzioni. Sullo scenario *Private Cloud* saranno quindi utilizzabili al momento della disponibilità dell'infrastruttura. La NewCo si farà carico di effettuare gli aggiornamenti dei prodotti, seguendone il relativo ciclo di vita;
- soluzioni *Open Source* disponibili sulla piattaforma Oracle Dedicated Region Cloud@Customer seguiranno il *provisioning* delle relative installazioni. Saranno quindi fin da subito elementi a catalogo che gli utenti potranno utilizzare;
- soluzioni *Open Source* fornite da catalogo su installazioni Google Distributed Cloud@Home seguiranno il *provisioning* delle relative installazioni, con immediata disponibilità per i fruitori dei servizi;
- la soluzione FASTcloud Container è un prodotto già disponibile; pertanto, sarà possibile utilizzarlo una volta effettuato il *provisioning* degli ambienti infrastrutturali.

La scelta di dotare il PSN di tecnologie *Open Source* nasce dall'esperienza pluriennale delle società facenti parte dell'Offerente; esperienza che ha portato nel tempo ad utilizzare tali tecnologie quali componenti abilitanti la realizzazione di servizi *cloud* privati per aziende clienti di tutte le dimensioni.

Ricade nell'ambito dei progetti *Open Source* la piattaforma FASTcloud Container, sviluppata da Fastweb per rispondere all'esigenza di una piattaforma di orchestrazione di contenuti containerizzati e per offrire ai clienti un'esperienza interamente *cloud native*. La piattaforma è già presente sul mercato e permette la realizzazione di servizi PaaS/CaaS su tecnologia *container* per clienti di tipo "*Enterprise*", con modalità di fruizione dedicata o condivisa delle risorse infrastrutturali. Per l'implementazione di alcune *feature* distintive sono stati utilizzati progetti sviluppati dalla *community* in ambito *Open Source*, come ad esempio per

l'implementazione della funzionalità di *multi-tenancy*, resa disponibile tramite il progetto *Capsule*.

### 1.6.2 La *suite* OpenStack – OpenShift

Un'importante scelta tecnologica per l'affiancamento di soluzioni *Open Source* alle soluzioni licenziate nel PSN è la *suite* OpenStack/OpenShift, supportata dal ***partner*** strategico Red Hat. Fastweb ha una partnership con Red Hat consolidata negli anni ed utilizza tecnologie Red Hat per numerose soluzioni negli ambiti di *Cloud* Privato e *Software Defined Storage*. Nel 2020 Fastweb ha stipulato la *partnership* Red Hat EMEA Certified Cloud & Service Provider (CCSP) posizionandosi come *partner* di livello *Advanced*; pertanto, come *regional partner* può offrire a terze parti prodotti basati su tecnologie Red Hat, negli ambiti del *Public Cloud*, *managed* services, *hosting* e/o *outsourcing*.

Red Hat OpenStack (RHOSP) è una tecnologia *Open Source* utilizzata per la realizzazione di servizi infrastrutturali IaaS in *cloud* privato, alimentata da un'ampia comunità di sviluppo e che garantisce un supporto - offerto dalla società Red Hat - di livello idoneo per una fornitura in ambito *Enterprise* e per servizi *mission critical*. OpenStack è una soluzione solida e completa che offre funzionalità che permettono la realizzazione di servizi infrastrutturali e di *cloud* privato, scalabili e flessibili, oltre a fornire tutti gli strumenti integrati per la gestione, l'esercizio e la sicurezza dei carichi di lavoro.
Di seguito le principali caratteristiche e funzionalità della piattaforma OpenStack:

- un ciclo di vita esteso che garantisce una soluzione affidabile e duratura che consente aggiornamenti continui e poco invasivi delle funzionalità, senza il rischio d'interruzione che può essere associato agli aggiornamenti più significativi;
- strumenti *Enterprise* e *user friendly* per la gestione centralizzata dell'infrastruttura e per le attività d'installazione e variazione di configurazioni;
- alta affidabilità dell'infrastruttura, garantita attraverso il riconoscimento dei guasti, l'evacuazione automatica degli *host*, il *fencing* dei nodi che evidenziano anomalie ed il riavvio automatico dei *workload* sui nodi disponibili;
- bilanciamento dell'infrastruttura, tramite processi automatici di redistribuzione dei carichi sui nodi e il riconoscimento dei nodi in stato di *failure*;
- la flessibilità di eseguire macchine virtuali ed applicazioni *cloud-native* in parallelo, ottenendo prestazioni analoghe a quelle di un equivalente *hardware* dedicato, grazie anche all'integrazione con OpenShift, la piattaforma Kubernetes offerta da Red Hat;
- ampia scelta tra le opzioni *hardware* fino a quelle di ultimissima generazione;
- un vasto ecosistema di prodotti e soluzioni terze integrate e certificate.

Red Hat OpenShift Container Platform (OCP) è invece una piattaforma di tipo *Enterprise* basata su Kubernetes e concepita per la realizzazione di servizi PaaS e CaaS *cloud* in ambito *Open Source*. OpenShift permette di automatizzare tutte le operazioni di gestione della tecnologia e offrire un'esperienza semplificata ed intuitiva per amministratori ed utilizzatori, allineandosi alle principali soluzioni di mercato. Di seguito le principali caratteristiche della piattaforma:

- utilizzo nativo del motore di orchestrazione *Open Source* Kubernetes e relative funzionalità, come ad esempio, gestione, scalabilità, schedulazione di applicazioni a *container*;
- sistema operativo specificatamente configurato ed ottimizzato sulla base di Red Hat Enterprise Linux che consente di soddisfare tutti requisiti di sicurezza;

- installazione per diversi ambiti: *bare metal*, VMware Vsphere, Red Hat *Virtualization* (KVM), OpenStack, compresi i principali *cloud provider* – per supportare sia scenari *Private Cloud* che *Public Cloud*;
- disponibilità di un *marketplace* di software *Enterprise* certificato, pronto per essere installato in una logica PaaS;
- possibilità di creare applicazioni con linguaggi/strumenti desiderati ed eseguirne il *deployment* attraverso le immagini dei *container*;
- controllo semplificato dei *deployment* e possibilità di standardizzare il flusso di lavoro degli sviluppatori, supportare svariati ambienti ed agevolare l'integrazione continua parallelamente ad una gestione automatizzata delle *release*.

Con la *suite* OpenStack ed OpenShift, l'Offerta si dota di un'architettura basata su *Open Source*, allineata tecnicamente e funzionalmente con i prodotti di riferimento – anche basati su licenza – per il mercato delle soluzioni *Private Cloud* e *Public Cloud*.

### 1.6.3 Miglioramento con tecnologie *Open Source* nell'ambito dei servizi *Private Cloud*

L'offerta dei servizi *Private Cloud* del PSN, a latere delle soluzioni proprietarie (ad esempio, quelle dello *stack* VMware), include la possibilità per le PA utenti di adottare uno *stack* tecnologico completamente *Open Source*, basato sulla combinazione delle tecnologie OpenStack ed OpenShift.
Tra le soluzioni basate su *Open Source*, le PA utenti potranno trovare servizi *Private Cloud* IaaS, PaaS, CaaS.

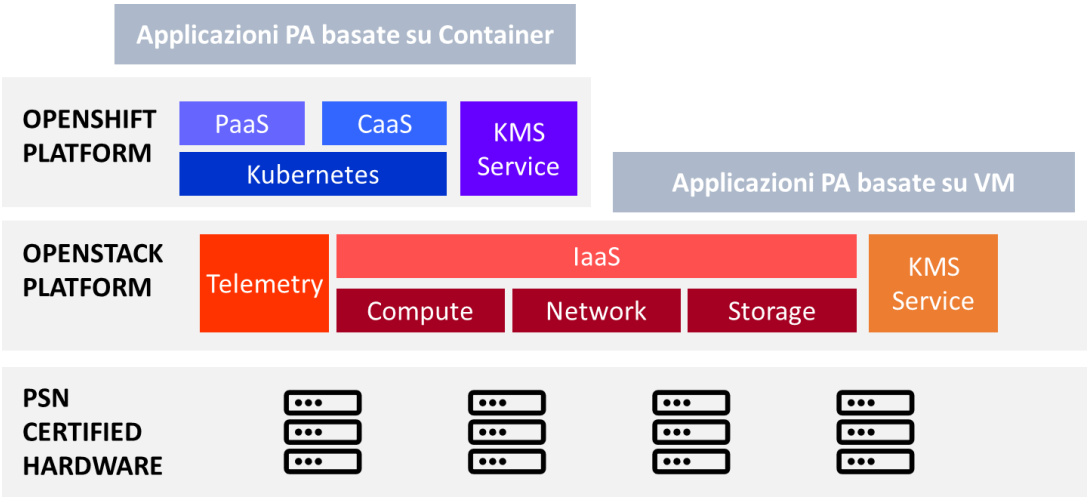



*Figura 3: Combinazione OpenShift e OpenStack*

La piattaforma OpenStack è destinata all'erogazione dei servizi di infrastruttura virtuale (ad esempio, *server*, macchine virtuali, risorse di archiviazione e *networking*) in linea con tutti i requisiti tecnici, gestionali operativi e di sicurezza propri del PSN:

I servizi IaaS sono disponibili in due modalità di erogazione differenti:

- IaaS *Shared*: infrastruttura (*hardware*, *network* e *storage*) virtualizzata e condivisa in grado di ospitare le applicazioni in carico alla PA;
- IaaS *Private*: infrastruttura (*hardware*, *network* e *storage*) virtualizzata e dedicata in grado di ospitare le applicazioni in carico alla PA.

Nella piattaforma OpenStack, le PA avranno la possibilità di gestire le risorse IaaS attraverso *dashboard* grafiche o linea di comando che permetteranno di creare, controllare ed automatizzare le risorse. La soluzione di cui all'Offerta metterà a disposizione anche un ampio *set* di API utili ad aumentare il grado di interoperabilità con le soluzioni di gestione esterna (anche basate su licenza) ed a facilitare l'interazione con sistemi di *cloud management* e di *cloud automation* adottate dalla PA utente.

Il seguente diagramma (Figura 4: I servizi principali di OpenStack) fornisce una panoramica di alto livello dei servizi principali di OpenStack e delle loro reciproche relazioni.

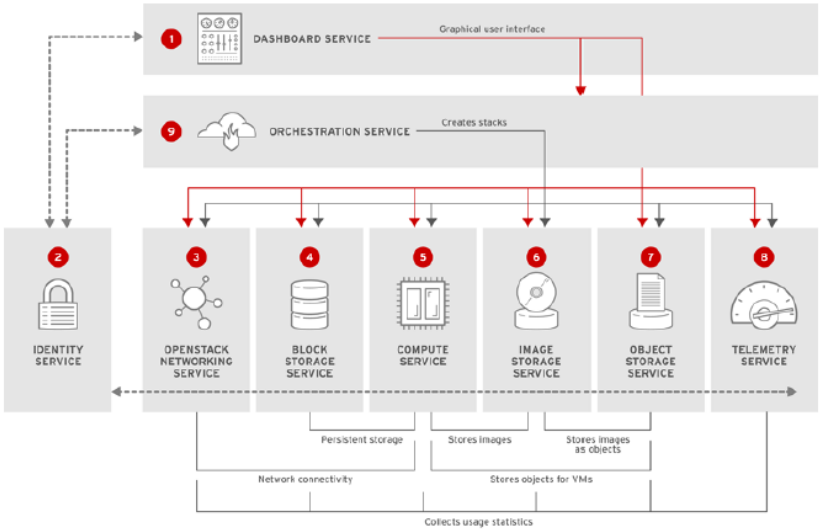



*Figura 4: I servizi principali di OpenStack*

Si aggiungono a quelli presenti in figura altri servizi trasversali, quali Barbican per la gestione delle chiavi ed Octavia per il *Load Balancing-as-a-Service*.

I servizi offerti su piattaforma OpenStack, come tutti i servizi del PSN, garantiranno i livelli definiti di disponibilità, lavorando sulle *Availability Zone* definite per le due regioni del PSN. Gli elementi di controllo, così come i carichi di lavoro, saranno anch'essi distribuiti tra le differenti *Availability Zone* delle regioni del PSN, in modo da rispondere agli obiettivi di continuità operativa.

L'erogazione dei servizi PaaS e CaaS si basa sull'utilizzo della piattaforma OpenShift, nativamente supportata da OpenStack. L'integrazione delle due piattaforme garantisce alle PA uno *stack* tecnologico completamente *Open Source* per la fruizione dei servizi di *Private Cloud*. Si avrà in tal modo un'architettura flessibile per le applicazioni *cloud-native* e containerizzate, con grandi capacità di scalabilità e adattamento ai carichi di lavoro.

Di seguito, un esempio di servizi PaaS resi disponibili dal *Private Cloud* e realizzati a partire da *stack Open Source*: DBaaS (sia relazionali che NOSQL), *BigData* (Datalake, EventQueue, ETL), AI/ML, IAM con immagini certificate fornite da Red Hat e/o da *Partner* terzi. Molte di queste immagini sono a loro volta generate da progetti *Open Source* ed aggiunte al catalogo dopo opportuna certificazione.

Nella piattaforma OpenShift Container Platform (OCP), le PA utenti troveranno una soluzione completa ed intuitiva, per la gestione e l'orchestrazione dei servizi CaaS e PaaS.
OCP offre tra l'altro:

- una *Container runtime* (CRI-O) in cui le applicazioni ed i servizi degli utenti finali vengono gestiti come *container* distribuiti in POD (raggruppamento di *container*);
- la gestione approfondita del *networking*, che fa leva anche sul concetto *Software-defined networking* (SDN) utilizzata per unificare e controllare attraverso *policy* le comunicazioni tra i POD all'interno del *cluster* OCP;
- l'utilizzo nativo di *Operator*, metodo di *packaging* per applicazioni native Kubernetes;
- la disponibilità di Red Hat OpenShift Registry, un registro integrato che garantisce l'utilizzo e la condivisione delle immagini utilizzate dai *container*;
- la disponibilità di *persistent storage* per le applicazioni che lo richiedano;
- gli strumenti di *ingress control,* che permettono l'accesso dall'esterno alla piattaforma ed ai suoi servizi interni tramite richieste HTTP/HTTPS via TLS;
- le soluzioni per l'autenticazione, l'autorizzazione (RBAC), le soluzioni di monitoraggio e *logging*.

#### *1.6.3.1 La sicurezza applicativa e dei dati nella soluzione Open Source*

La combinazione delle due piattaforme OpenStack ed OpenShift garantisce alle PA utenti un contesto di gestione dei propri dati, delle proprie chiavi di sicurezza e dei certificati basata completamente su soluzioni *Open Source,* idoneo per una fornitura *Enterprise* e per servizi *mission critical*.
Nello specifico OpenShift declina il tema sicurezza rispetto alle seguenti direttrici:

- Sicurezza del sistema Operativo: utilizzo del sistema operativo CoreOS, tra i più sicuri sul mercato. A differenza di altri sistemi operativi, con CoreOS i *team* operativi hanno la possibilità di modificare/configurare un *set* minimo di parametri. OpenShift viene nativamente ingegnerizzato per essere distribuito su CoreOS;
- Sicurezza del *layer* Kubernetes: il *database* Etcd, che contiene lo stato di tutti i *workload* all'interno di Kubernetes, viene criptato con chiavi che possono essere gestite dal servizio *Key Management* di OpenStack o da HSM esterni. Inoltre, la comunicazione tra *container* che risiedono su nodi di OpenShift differenti può essere resa sicura attraverso l'utilizzo di canali IPsec;
- Sicurezza del *layer* di *Software-Defined Storage*: come mostrato nella figura seguente, OpenShift supporta la crittografia dei volumi persistenti attraverso l'utilizzo di un servizio KMS esterno, come ad esempio HashiCorp Vault, che può essere integrato con la soluzione HSM di Thales;

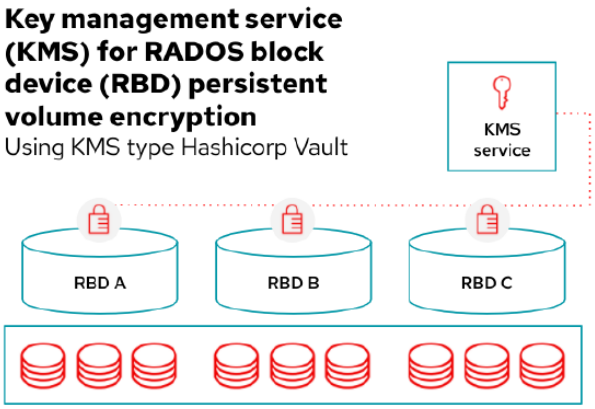



*Figura 5: OpenShift KMS*

- Sicurezza delle *Container Image*: OpenShift mette a disposizione un elevato numero di immagini *container* certificate tra le quali: Linux Operating System, Apache Web Server, JBoss Enterprise Application Platform, PostgreSQL, e Node.js. Queste immagini sono costruite a partire da codice sorgente *Open Source* e validato dagli specialisti Red Hat, che ne eseguono un controllo ed un monitoraggio continuo di qualità e sicurezza.

La gestione delle chiavi di crittografia, nella piattaforma Open Source proposta dall'Offerente, è completamente in mano al personale della NewCo e prevede l'integrazione tra i CSP con HSM esterni alle loro soluzioni, localizzati presso i siti del PSN (ad es. Barbican, il servizio di Key Management Open Source nativo in OpenStack, che potrà essere sfruttato per la gestione centralizzata dei certificati, delle chiavi di cifratura e delle password utilizzate dai servizi). Sono supportati i seguenti scenari d'utilizzo:

- Chiavi di crittografia simmetrica - usate per la crittografia di volumi *Block Storage* (Cinder), la crittografia dei dischi effimeri e la crittografia *Object Storage* (Swift), tra gli altri;
- Chiavi asimmetriche e certificati – utilizzati, tra l'altro, per la firma e la verifica.

### 1.6.4 Miglioramento con tecnologie *Open Source* nell'ambito dei servizi *Hybrid Cloud* on PSN *Site* e *secure Public Cloud*

Il miglioramento con tecnologie *Open Source* dei servizi di tipo *Hybrid Cloud on PSN Site* si consegue attraverso l'adozione della piattaforma OpenShift configurata ed installata all'interno delle soluzioni Azure HCI ed AWS Outposts, ospitate nei DC del PSN. Attraverso l'adozione della piattaforma si conseguono due risultati:

- la possibilità di erogare servizi PaaS e CaaS di tipo *Open Source* veicolati tramite OpenShift su queste architetture;
- l'opportunità di costruire una architettura ibrida verso il mondo del *cloud* privato PSN, che sia orchestrata con un prodotto di gestione e orchestrazione totalmente locale ai DC del PSN, che offra anche una gestione delle chiavi in locale attraverso la piattaforma *Open Source* stessa.

La piattaforma OpenShift installata sulle soluzioni *on-premise* dei *Cloud Provider* permetterà di creare e gestire servizi PaaS e CaaS di tipo *Open Source* sfruttando template ed immagini messi a disposizione *ad-hoc* per le PA utenti, gestiti ed aggiornati dal PSN.
Tra i servizi *Open Source* disponibili si citano i seguenti:

- DBaaS, servizi di *Database-as-a-Service* basati su tecnologie *Open Source* come:
  - MongoDB;
  - PostgreSQL;
  - MySQL;
  - Redis;
  - ElasticSearch;
- *Stream Analysis*, servizi di *Event Message* basati su tecnologie *Open Source* come:
  - Apache Kafka;
  - ActiveMQ;
- IAM: servizi di *Access management* basati su tecnologie *Open Source* come KeyCloak;
- AI/ML: Immagini containerizzate per l'esecuzione di modelli di Intelligenza Artificiale e *Machine Learning;*
- CaaS: ambiente d'esecuzione containerizzato supportato da strumenti DevOps e di collaborazione, nativi della piattaforma *Open Source*.

Per erogare questi servizi si prevede di installare, sulle soluzioni on *premise* dei *cloud provider*, *cluster* OpenShift destinati alle PA utenti, che potranno essere anche configurati su *hardware* dedicato per garantire una completa segregazione logica e fisica delle applicazioni. Alle PA utenti, che necessitano di un'elevata quantità di risorse computazionali, potrà anche essere dedicato l'intero *cluster* OpenShift. La gestione ed il *capacity management* del *cluster*, sia esso dedicato o condiviso e la modifica delle risorse *hardware* assegnate, saranno di responsabilità della NewCo e potrà essere richiesta dalle PA utenti attraverso il processo di *service request*.

La realizzazione dell'architettura ibrida verso il mondo del *Private Cloud* PSN si ottiene installando diversi *cluster* OpenShift sulla componente *cloud* privata e sulle soluzioni *on-premise* dei *Cloud Provider*, integrando il servizio di gestione *Open Source* RHACM (Red Hat *Advanced Cluster Management*) con cui è possibile:

- gestire i *cluster* distribuiti sulle soluzioni *private*, HCI e Outposts;
- monitorare le risorse computazionali del *cluster* ovunque siano installati;
- gestire il ciclo di vita e l'installazione delle applicazioni;
- accedere ad un pannello di controllo unico in *dashboard* grafiche o con linea di comando.

Con l'adozione di RHACM, le PA utenti potranno gestire le risorse del mondo PSN *Private Cloud* e *Hybrid Cloud on PSN Site* con uno strumento centralizzato, che rende omogenea l'operatività ed allinea i processi di sviluppo delle applicazioni secondo il paradigma di *cloud* ibrido. La soluzione permetterà, tra l'altro, di agevolare la migrazione dei *workload* applicativi tra i due contesti qualora richiesto dalle esigenze di carico o di sicurezza.

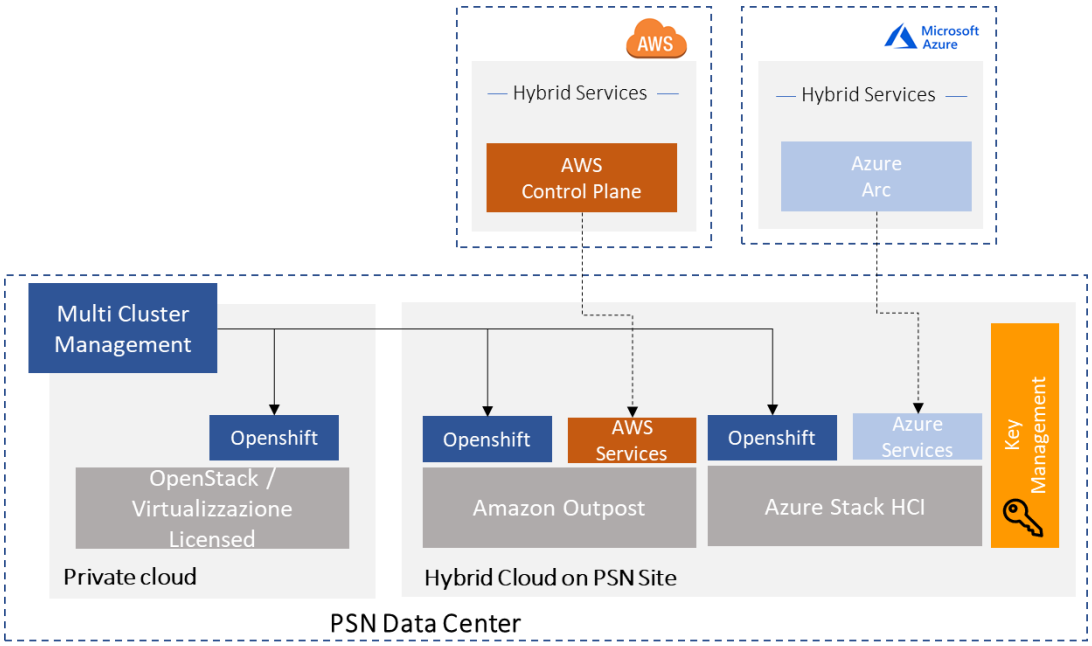



*Figura 6: Openshift nella architettura Hybrid Cloud on PSN Site*

Stante il profilo di sovranità che contraddistingue i servizi del PSN, è importante evidenziare come queste funzionalità di gestione ed orchestrazione centralizzate, anche nella componente di *Control Plane*, siano installate all'interno dei DC del PSN, sotto la sua unica responsabilità anche operativa.

La soluzione Red Hat Advanced Cluster Manager è in grado di gestire *cluster* installati anche sulle risorse del *Secure Public Cloud*. Può, quindi, essere utilizzata come elemento di orchestrazione comune tra lo scenario *Hybrid on PSN Site* e lo scenario *Secure Public Cloud*, consentendo il riutilizzo di template e risorse.

Relativamente alla sicurezza della soluzione, valgono le stesse considerazioni del paragrafo precedente, anche in merito all'utilizzo di un servizio di gestione esterna delle chiavi di cifratura.

### 1.6.5 Miglioramento con tecnologie *Open Source* nell'ambito dei servizi *Public Cloud* PSN *Managed*

Il miglioramento con tecnologie *Open Source* dei servizi di tipo *Public Cloud* PSN *Managed* si consegue selezionando e mettendo a disposizione sulle due soluzioni sviluppate con i *partner* operatori del *Cloud* (ma non solo) – Google Distributed Cloud Hosted e Oracle Dedicated Region Cloud@Customer – componenti e servizi che si basano su tecnologia *Open Source*.

Questi servizi sono erogati in modalità PaaS e si affiancano ai servizi nativi offerti dai CSP nell'ambito *Public Cloud* PSN *Managed*. La fornitura dei servizi in modalità PaaS rende la fruizione del servizio semplificata per le PA utenti e garantisce un processo di attivazione rapido evitando complessità operative.

Tra i servizi *Open Source* resi disponibili dalla soluzione Google Distributed Cloud Hosted si citano:

- DBaaS, servizi di *Database-as-a-Service* basati su tecnologie *Open Source* come:
  - MongoDB;
  - Redis;
  - ElasticSearch;
- *BigData*, servizi basati su tecnologie *Open Source* come:
  - Hadoop;
  - Kafka;
- CaaS: ambiente di esecuzione containerizzato basato su Kubernetes GKE.

Tra i servizi *Open Source* messi a disposizione dalla soluzione Oracle Dedicated Region Cloud@Customer si citano:

- *BigData services*:
  - Apache Hadoop Ecosystem (Hadoop, Hive, Spark, ecc.);
  - Apache Kafka;
- DBaaS:
  - MySQL;
  - Apache HBase;
- CaaS: ambiente di esecuzione containerizzato basato su Kubernetes;
- *Resource Manager*:
  - Terraform.

Per la componente CaaS, inoltre, l'Offerente affianca alle soluzioni proposte in ambito *Public Cloud* PSN *Managed,* la piattaforma FASTcloud Container, una soluzione sviluppata interamente da Fastweb con tecnologia completamente *Open Source* per offrire un'esperienza Kubernetes "nativa".

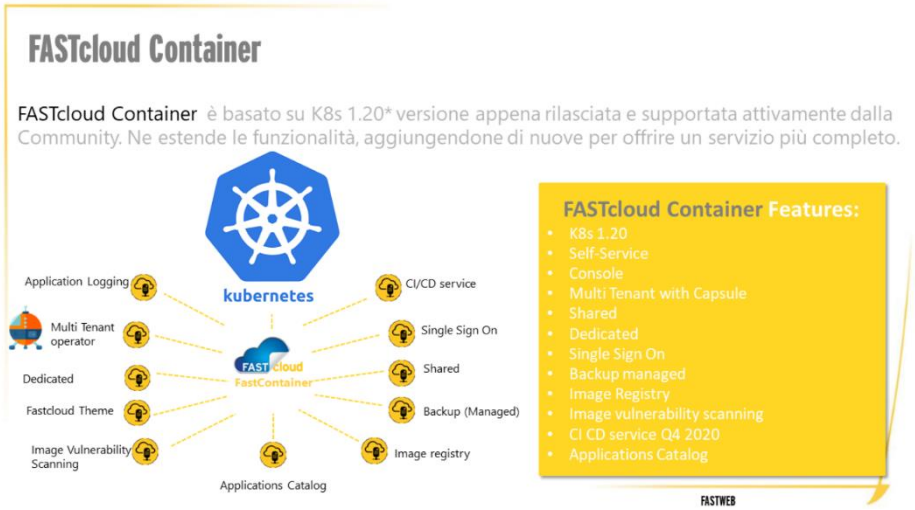



*Figura 7: FASTcloud container*

Di seguito si citano ad esempio alcune *feature* implementate dalla soluzione FASTcloud Container:

- *Dashboard Console* (OKD based);
- SSO con 2FA (Keycloak);
- *Multitenancy* (Capsule Operator);
- *Image Registry* e servizio di *vulnerability scan* (Harbor);
- *Application Logging* (Grafana/Loki);
- *Application Catalog* (Kubeapps);
- CI/CD *Service* - (Jenkins/Argo-CD);
- *Backup* gestito - (Velero).

Nonostante la declinazione *Open Source* della piattaforma, il supporto è garantito da Canonical per la parte di sistema operativo e Kubernetes e da fornitori esterni per la parte di sviluppo/*maintenance* di nuove *feature*.
Di seguito riportiamo, per chiarezza, le due proposizioni attualmente disponibili per la suddetta soluzione:

- FASTcloud Container **Shared** *Container-as-a-Service*, con nodi computazionali (*Worker Node*) e connettività condivisi;
- FASTcloud Container **Dedicated** *Container-as-a-Service*, con nodi computazionali (*Worker Node*) dedicati e connettività dedicata.

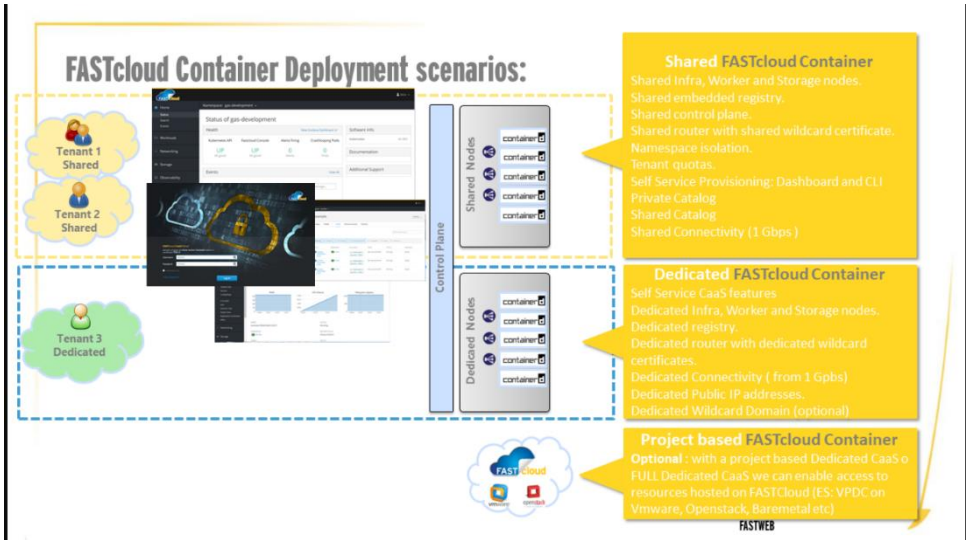



*Figura 8: FASTcloud container deployment scenarios*

Il servizio di *Control Plane* Kubernetes è ospitato su nodi specifici (*Master Node*), ed è erogato come unico "servizio" per tutti i *Tenant*, in modo da ottimizzare le risorse computazionali e le attività operative e di manutenzione.

## 1.7 ID CRITERIO:7 –TABELLARE - MIGLIORAMENTO DEL VALORE SOGLIA DELL'INDICATORE DI QUALITÀ IQ04 PARI A NUMERO 5 RILIEVI

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|
| **7** | Tabellare | Tecnologie *Cloud* | Miglioramento dell'indicatore di qualità IQ04 | Miglioramento del valore soglia dell'indicatore di qualità IQ04 pari a numero 5 rilievi | 0,2 punti per ogni unità inferiore a 5 | **1** |

L'interazione tra la NewCo e le PA utenti dovrà essere caratterizzata da trasparenza, efficacia ed efficienza. In quest'ottica, la NewCo opererà minimizzando il più possibile le mancate approvazioni dei documenti per facilitare le PA utenti nel loro percorso di adozione dei servizi del PSN.
L'Offerente propone, pertanto, **di migliorare il valore soglia dell'indicatore IQ04, pari a 5 rilievi nella documentazione di gara, portandolo a 0 rilievi**.

Miglioramento del valore soglia IQ04

| Punteggio indirizzato dall'Offerente = 1 punto | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore soglia IQ04 = 5 rilievi | Valore soglia IQ04 proposto dall'Offerente = 0 rilievi |

Per garantire il rispetto della soglia proposta, la NewCo sarà dotata dei seguenti elementi:

- Adozione di **template** predefiniti per i documenti basilari, disegnati in ottica di trasparenza e chiarezza verso le PA utenti;
- Processo di **miglioramento continuo** dei template in base ai *feedback* ricevuti dalle PA;
- **Meccanismi approvativi**, interni alla NewCo, per la validazione dei documenti prodotti pre-condivisione con le PA utenti.

## 1.8 ID CRITERIO:8 – TABELLARE - MIGLIORAMENTO DEI SEGUENTI VALORI: RTO ATTESO DELL'INDICATORE DI QUALITÀ IQ11 PARI A 30 MINUTI, RPO *TARGET* DELL'INDICATORE DI QUALITÀ IQ12 PARI A 1 MINUTO, RTO SU DIVERSA *REGION* ATTESO DELL'INDICATORE DI QUALITÀ IQ13 PARI A 4 ORE, RPO SU DIVERSA *REGION TARGET* DELL'INDICATORE DI QUALITÀ IQ14 PARI A 30 MINUTI

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| **8** | Tabellare | Tecnologie *Cloud* | Miglioramento dell'indicatore di qualità IQ11, IQ12, IQ13 e IQ14 | Miglioramento dei seguenti valori:<br>- RTO atteso dell'indicatore di qualità IQ11 pari a 30 minuti<br>- RPO target dell'indicatore di qualità IQ12 pari a 1 minuto<br>- RTO su diversa Region atteso dell'indicatore di qualità IQ13 pari a 4 ore<br>- RPO su diversa Region target dell'indicatore di qualità IQ14 pari a 30 minuti | **1 punto** | per valori di RTO atteso pari a 15 minuti, RPO target pari a 40 secondi, RTO su diversa Region atteso pari a 1 ora e RPO su diversa Region target pari a 20 minuti | **2** |
| | | | | | **2 punti** | per valori di RTO atteso pari a 10 minuti, RPO target pari a 30 secondi, RTO su diversa Region atteso pari a 30 minuti e RPO su diversa Region target pari a 15 minuti | |

La tabella seguente sintetizza la proposta dell'Offerente in relazione al criterio 8 che, come risulta dai valori proposti, rappresenta un **evidente miglioramento rispetto ai parametri previsti nel Documento contenente la descrizione dei servizi, capitolo 2**.
Nei paragrafi seguenti sono riportati i dettagli tecnici alla base della miglioria proposta.

Miglioramento dell'offerta mediante il miglioramento degli indicatori di qualità IQ11, IQ12, IQ13 E IQ14

| Punteggio indirizzato dall'Offerente = 2 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valori Base:<br>• RTO IQ11 < 30 min<br>• RPO IQ12 < 1 min<br>• RTO IQ13 < 4 ore<br>• RPO IQ14 < 30 min | Valori dell'Offerente:<br>• RTO IQ11 < 5 min<br>• RPO IQ12 < 15 sec<br>• RTO IQ13 < 25 min<br>• RPO IQ14 < 10 minuti |

### 1.8.1 Miglioramento dell'indicatore di qualità IQ11, IQ12, IQ13 e IQ14

L'Offerente metterà a disposizione un'infrastruttura distribuita sul territorio nazionale, del tutto coerente con quanto previsto nella documentazione di gara ed in particolare, dal Progetto di fattibilità. Questa sarà **organizzata secondo una strategia ben consolidata di *Business Continuity*** e mediante un'infrastruttura tecnologica tale da garantire elevate capacità di replica e ripristino dei sistemi, oltre ai massimi *standard* qualitativi in termini di affidabilità, disponibilità e sicurezza, allineandosi alle pratiche più consolidate a livello globale.
L'infrastruttura fisica fornita dall'Offerente, assieme ad un *Global Control Plane*, permetterà di gestire trasparentemente l'istanziazione, la gestione e l'erogazione di servizi da diverse *Region* ed *Availability Zone*. Con tale configurazione, ciascuna PA utente sarà autonoma nel gestire i propri applicativi, dati e nell'implementare le proprie *policy*/processi di DR, *Backup* e/o BC in base all'esigenza ed ai requisiti di ciascun applicativo in perimetro.

#### *1.8.1.1 Strategia di sito*

L'Offerente propone una strategia di sito basata su ***Region* di alta affidabilità**. Nello specifico, in coerenza con quanto previsto nel Progetto di fattibilità, si prevedono due *Region* (*Region Nord* e *Region Centro-Sud*, di riferimento anche per le isole), localizzate nei baricentri delle dorsali di connettività che collegano le PA utenti. Questo posizionamento garantisce, a livello di rete, la più equa distribuzione delle distanze per una massimizzazione delle *performance* - tra le varie PA utenti sul territorio nazionale e la loro *Region* di riferimento.
Ciascuna *Region* di alta affidabilità prevede una coppia di DC, ognuno dei quali implementa una *Availability Zone*. Le *Availability Zone* saranno isolate e fisicamente separate da una connettività di lunghezza inferiore ai 100km, per garantire decorrelazione del rischio di disastro, preservando al contempo la possibilità di allineamento in modalità sincrona dei dati.

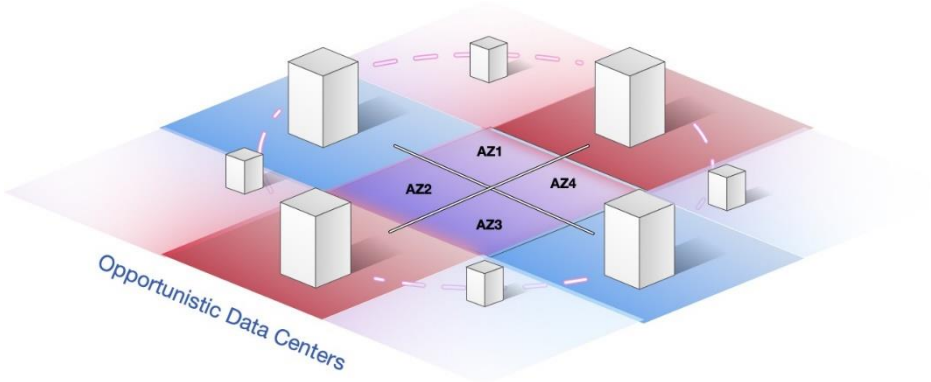



*Figura 9: Strategia di sito*

Le *Region* sono interconnesse tra loro attraverso l'utilizzo della rete del PSN, che garantisce massime prestazioni di comunicazione mediante collegamenti ridondati, nell'accesso ai siti e nel percorso, garantendo inoltre velocità trasmissive elevate in modo tale da identificare la coppia di *Availability Zone* di *Region* come un unico DC virtuale.
L'attivazione delle quattro *Availability Zone* e la loro crescita verso il regime di funzionamento avverrà progressivamente.

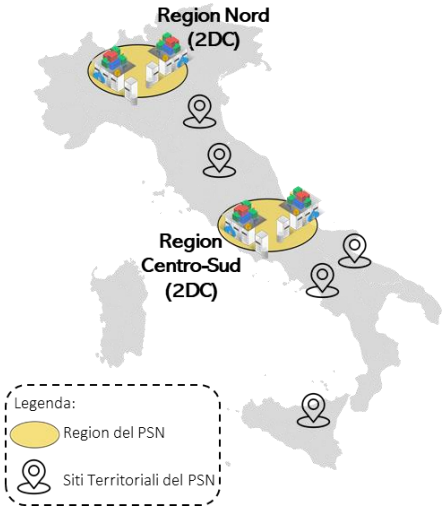



*Figura 10: Region ad alta affidabilità*

Oltre alle quattro *Availability Zone* di *Region*, il PSN opzionalmente potrebbe offrire dei **siti territoriali attrezzati** - noti anche come *Edge* - distribuiti sul territorio nazionale per ospitare i sistemi delle PA utenti che necessitino di avere un DC fisicamente molto prossimo, pur conservando il medesimo grado di sicurezza ed affidabilità garantiti dal PSN.
I siti attrezzati territoriali sono ritenuti una leva molto importante per abilitare una migrazione rapida ed esaustiva delle applicazioni della PA utente, in particolare in due casistiche:

- migrazione di applicazioni con architetture "*legacy*" (es: *client-server*), nate per funzionare in ambiente locale e che potrebbero soffrire della remotizzazione di una componente dello *stack* applicativo. In questo caso, una *relocation* del *server* in sito molto prossimo potrebbe rendere possibile un primo passaggio al PSN in attesa di una modernizzazione dell'applicativo;
- migrazioni di applicazioni molto sensibili alla latenza, che siano collocate presso PA utente, che soffrano transitoriamente di una non idonea *performance* nella rete di accesso (*digital divide*). In questi casi il *rehosting* presso il sito territoriale di una componente computazionale potrebbe compensare il difetto di *performance*, che si rischierebbe di soffrire forzando una migrazione verso le *Region*.

I siti territoriali, oltre a essere un fattore abilitante per la migrazione degli applicativi, aprirebbero il PSN verso un modello *Cloud-&-Edge*, che potrebbe essere molto importante per i prossimi passi dell'evoluzione digitale delle PA utenti. Si pensi, ad esempio, a servizi tipo il controllo del territorio basato sulla AI, l'assistenza domiciliare remota, come la tele-medicina - espressamente prevista nella Missione 6-Sanità del PNRR – ed i vari casi d'uso del mondo *smart-city*.
Ciascuna PA sarà in grado di fruire dei servizi *Cloud* offerti dal PSN andando ad istanziare ed utilizzare risorse in una qualunque *Region* ed *Availability Zone*. Nel caso in cui sia necessario dover connettere tra loro servizi geograficamente dislocati su più *Region*/*Availability Zone*, sarà possibile definire un *Network Layer* logico (secondo il paradigma *Software Defined Network*) tale da astrarre l'effettiva dislocazione delle istanze.

#### *1.8.1.2 Continuità di servizio*

Obiettivo del PSN è garantire i livelli massimi di continuità del servizio e gli opportuni meccanismi e processi di prevenzione, mitigazione e recupero da qualunque tipo d'incidente o evento disastroso che rischi di affliggerne l'infrastruttura.
I DC del PSN saranno quindi basati su tecnologie ridondate rispetto a forniture ed equipaggiamenti. I DC che costituiscono una *Region* di alta affidabilità sono alimentati, equipaggiati e serviti da reti, sistemi e processi indipendenti tra di loro, per minimizzare il rischio di incidente congiunto, attraverso una connessione tramite reti di telecomunicazione a ridondanza multipla con bassissima latenza.
I DC prevedono meccanismi di replica *intra-Region* (tra *Availability Zone*) ed *extra-Region* al fine di garantire elevati *standard* di resilienza e di abilitare scenari di DR/BC per i diversi applicativi delle PA utenti. In particolare, la tecnologia utilizzata permetterà di effettuare una replica sincrona tra *Availability Zone* della stessa *Region* ed una replica asincrona tra *Availaibility Zone* appartenenti a *Region* diverse.

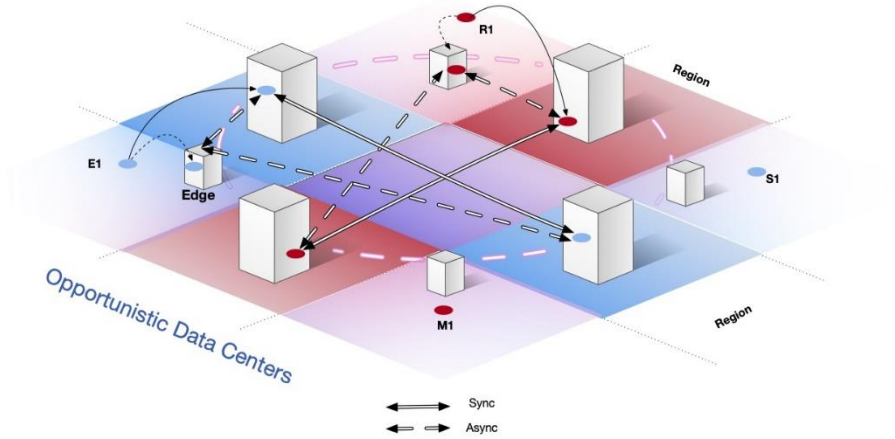



*Figura 11: Repliche sincrone e asincrone tra Availability Zone*

#### 1.8.1.2.1 Multi-site replica

Oltre alle repliche *intra-Region* ed *extra-Region*, la soluzione proposta dall'Offerente assicura la possibilità di replica su tutti i DC del PSN. Questa tipologia di configurazione abiliterà scenari in cui è richiesta una disponibilità del dato molto elevata ed al tempo stesso, renderà possibile l'utilizzo del dato dalla *Availability Zone* più prossima all'applicativo, in modo tale da ridurre drasticamente i tempi di latenza.
I servizi erogati dalla NewCo saranno certificati ISO22301 e garantiranno l'applicazione degli *standard* e delle pratiche di riferimento in termini di BC e continuità operativa. L'elevata affidabilità dei servizi e delle infrastrutture del PSN viene garantita da un piano di BC, anche personalizzabile in base alle esigenze delle singole PA utenti, per minimizzare l'indisponibilità dei sistemi (*Recovery Time Objective*) e preservare il dato da ogni perdita (*Recovery Point Objective*).
I DC saranno interconnessi tra loro mediante apparati DWDM (*Dense Wavelength Division Multiplexing*), con percorsi in fibra diversificati ad elevata capacità (N x 100 Gbps criptati); la tecnologia DWDM consente di ridurre i valori di latenza a beneficio del complessivo RTO, sia in ambito metropolitano tra i DC, sia in ambito nazionale tra le *Region*.
I DC, inoltre, saranno interconnessi al *Backbone* IP in modalità "*Dual Homing*" verso dei PoP (*Point of Presence*), geograficamente separati in differenti siti tecnologici; l'interfacciamento verso la rete IP consente di erogare servizi ad elevata affidabilità alle PA utenti nelle seguenti modalità:

- privata: tramite una rete VPN MPLS per il collegamento verso sedi periferiche della PA utente;

- pubblica: tramite rete *Internet*.

L'interconnessione in ambito nazionale è realizzata tramite la rete di Lunga Distanza Fastweb, che rende disponibili tre percorsi differenti. Per garantire la comunicazione tra la *Region* Nord e la *Region* Centro-Sud, vengono utilizzati meccanismi di protezione e resilienza dei percorsi, che consentono valori di latenza RTT tra 10 e 15 ms in relazione al percorso utilizzato.
La disponibilità dello strato DWDM e del *Backbone* IP offre la massima flessibilità nella comunicazione verso i CSP, rendendo semplice definire sia connessioni dedicate ad elevate velocità (es. 10/100 Gbps) che connessioni condivise/*hosted* a velocità inferiori.

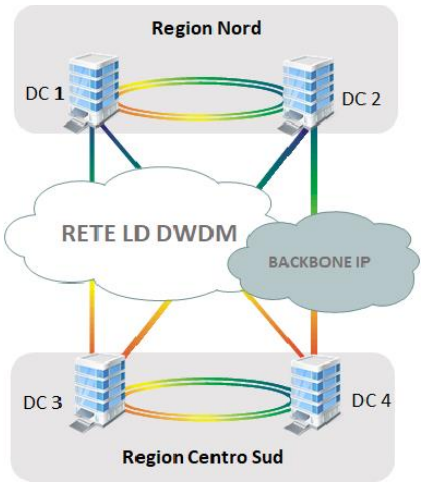



*Figura 12: Schema di interconnessione fra i DC*

Tutte le interconnessioni verso le reti geografiche sono governate dall'infrastruttura presente nei DC mediante tecnologia SDN, attraverso una piattaforma centralizzata che consente di governare l'infrastruttura di rete, automatizzandone le configurazioni e semplificandone la gestione sia in fase di *provisioning*, che di *assurance*.

#### *1.8.1.3 Miglioramento dell'indicatore di qualità IQ11 e IQ 12*

Per poter garantire i massimi livelli di continuità, l'Offerente propone, grazie all'utilizzo di strumenti *leader* di mercato in questo ambito, una configurazione di *High Availability* con replica sincrona dei dati ed un'estensione del *Layer* 2 di *networking* tra i DC all'interno della stessa *Region*. Questa configurazione sarà in grado di fornire una replica dei dati sincrona e trasparente all'interno delle due *Availability Zone* di *Region*, fornendo una soluzione tecnica tale da abilitare scenari di DR/BC per applicazioni *Mission Critical* richiedenti RTO/RPO molto bassi.

Con queste caratteristiche tecniche, l'Offerente propone i seguenti valori di RTO e RPO per gli indicatori IQ11 e IQ12:

| RTO | RPO |
|---|---|
| < 5 min | < 15 sec |

Questi livelli molto stringenti vengono erogati mediante l'utilizzo di tecnologie di storage "*best of breed*" tali da fornire:

- *Encryption end-to-end* ed *encryption* at *rest*;

- Configurazioni di *High Availability Active-Active*;
- *Thin Provisioning*;
- *Snapshot journaling*;
- HA *Active-Active Synchronous Replication* + DR *Asynchronous Replication*;
- *Automated Tiering*;
- Connettività a 32Gbps;
- Possibilità di *switch* da replica sincrona ad asincrona (e viceversa), in maniera non distruttiva;
- Gestione, monitoraggio, reportistica, *chargeback* e storicizzazione delle performance;
- Elevata resilienza dell'infrastruttura *storage*, con funzionalità garantite anche in caso di perdita considerevole di meccaniche;
- Virtualizzazione delle funzioni *storage*.

#### *1.8.1.4 Miglioramento dell'indicatore di qualità IQ13 e IQ14*

Oltre alla replica tra DC all'interno della stessa *Region*, è prevista la possibilità di replica del dato tra *Region* differenti. Questa replica viene effettuata in modalità asincrona a garanzia di un'elevata consistenza e sicurezza dei dati. Questa modalità di sincronizzazione permette di abilitare scenari di DR/BC tali da garantire l'operatività anche in caso di perdita di una *Region*.
In questo scenario di replica tra *Region*, i valori di RTO ed RPO che l'Offerente propone per i requisiti IQ13 ed IQ14 sono:

| RTO | RPO |
|---|---|
| < 25 min | < 10 min |

Inoltre, le caratteristiche relative agli apparati di *storage* e infrastrutturali potranno essere adattate in funzione della latenza, al fine di raggiungere soglie di RTO/RPO *target* significativamente inferiori a quelle richieste (es. RPO nell'ordine di pochi secondi).
A *latere* delle componenti tecniche e delle soglie di RTO/RPO raggiungibili tecnicamente, le tecnologie che l'Offerente utilizzerà forniranno la piena autonomia da parte delle PA utenti nel definire ed implementare le proprie strategie, piani e *policy* di BC/DR più consone per ciascun applicativo. Ciascuna PA utente potrà, ad esempio, definire specifici livelli di servizio al fine di catalogare gli applicativi in base alla criticità per il *business* (es. *Mission Critical*, *Business Critical*, etc.) ed all'RTO/RPO atteso, in modo tale da poter ottimizzare costi, risorse ed *availability*.
Oltre alla componente infrastrutturale, che abilita scenari a basso RPO, l'infrastruttura permetterà alle singole PA utenti di far leva su un'elevata capacità di automazione ed orchestrazione delle soluzioni di ripristino al fine di abbattere il valore di RTO per alcune famiglie di applicativi critici.

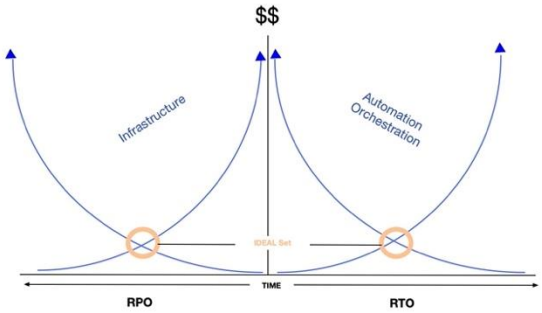


*Figura 13: RPO e RTO - Automation and Orchestration*

Queste capacità di automazione ed orchestrazione permetteranno di poter definire, in base al livello di famiglia di applicativi e di criticità, dei *template* di ripristino riutilizzabili da parte della PA per garantire la standardizzazione dei processi e l'applicazione di determinati livelli di RTO/RPO in base alla criticità del *workload*.

In aggiunta alla componente prettamente tecnica, l'Offerente prevede di erogare servizi professionali alle PA utenti, con il fine di supportare:

- la progettazione, la stesura e la manutenzione della componente infrastrutturale dei piani di BC e DR;
- la programmazione continua e l'esecuzione dei *test* di *Disaster Recovery*;
- la gestione della continuità infrastrutturale e del ripristino delle infrastrutture in caso di disastro.

Il servizio di *Vaulting & Backup* è indirizzato nel capitolo "2.3.4.1 Off-site Vaulting" del documento Annesso alla relazione tecnica.

## 1.9 ID CRITERIO:9 – TABELLARE - MIGLIORAMENTO DEI VALORI SOGLIA DELL'INDICATORE DI QUALITÀ IQ017 CON RIFERIMENTO AI TEMPI MASSIMI DI RISOLUZIONE IN ORE (PRIORITÀ 1 <= 4 ORE; PRIORITÀ 2 <= 8 ORE; PRIORITÀ 3 <=12 ORE)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 9 | Tabellare | Supporto | Miglioramento dell'indicatore di qualità IQ017 | Miglioramento dei valori soglia dell'indicatore di qualità IQ017 con riferimento ai tempi massimi di risoluzione in ore (Priorità 1 <= 4 ore; Priorità 2 <= 8 ore; Priorità 3 <=12 ore | **1 punto** | per Priorità 1 <= 3 ore; Priorità 2 <= 6 ore; Priorità 3 <= 9 ore | **2** |
| | | | | | **2 punti** | Priorità 1 <= 2 ore; Priorità 2 <= 4 ore; Priorità 3 <= 6 ore | |

In merito al criterio 9, l'Offerente propone le seguenti migliorie, meglio descritte nei paragrafi successivi. In particolare, l'Offerente propone una **significativa riduzione dei valori di soglia dell'IQ17** rispetto ai valori base, per tutte le classi di priorità previste:

Miglioramento dell'offerta mediante il miglioramento dell'indicatore di qualità IQ17

| **Punteggio indirizzato dall'Offerente = 2 punti** | |
|---|---|
| **Documentazione di gara** | **Miglioramento proposto dall'Offerente** |
| **Valori Base:**<br>• Priorità 1 <= 4 ore<br>• Priorità 2 <= 8 ore<br>• Priorità 3 <=12 ore | **Valori dell'Offerente:**<br>• Priorità 1 < = 2 ore<br>• Priorità 2 < = 4 ore<br>• Priorità 3 <= 6 ore |

### *1.9.1 Event Management*

#### *1.9.1.1 Gestione degli Eventi*

Lo scopo del processo di *Event Management* è quello di identificare, prioritizzare e classificare gli eventi riguardanti piattaforme e infrastrutture *cloud*, servizi, processi di *business* e sicurezza, e di stabilirne una risposta appropriata, in particolare definendo una soluzione **proattiva** alle cause che potrebbero portare a guasti, incidenti o disservizi.

Grazie ad una pronta rilevazione degli eventi, ad un efficiente sistema di generazione ed allo smistamento di notifiche e *ticket* supportati da strumenti di automazione (es. *autoticketing*, auto-*remediation*), il processo di *Event Management* è cruciale nel garantire i livelli di disponibilità infrastrutturale accordati con la PA utente (*Availability Management*).

Si definisce 'evento' un qualsiasi accadimento rilevabile o evidente che ha un significato per la gestione delle infrastrutture IT. Il processo di *Event Management* è costituito da:

- monitoraggio di tutti gli eventi che si verificano a livello infrastrutturale, rilevando e notificando condizioni di eccezione rispetto al funzionamento atteso. Include la scansione, la raccolta, la valutazione, la risposta e la reportistica di eventi relativi alle piattaforme e alle infrastrutture *cloud*;
- classificazione degli eventi infrastrutturali e delle tipologie di risposta agli eventi stessi;
- profilazione degli eventi per suddividerli in gruppi a seconda della loro origine e della risoluzione.

Solo gli eventi ritenuti significativi vengono opportunamente indirizzati: a tal proposito, la classificazione prevede apposite etichette (e.g. *information*, *warning* o *exception*), a seconda dell'impatto che l'evento genera sull'infrastruttura o piattaforma *cloud*.
La soluzione dell'Offerente prevista per il servizio di *Event Management* può essere così scomposta e descritta:

- *Host Monitoring:*
  - Tipologia degli *host*, piattaforme virtuali e fisiche;
  - *Target* del monitoraggio per ogni *host*:
    - Risorse HW: CPU, Memoria, *filesystem*, *log*, etc.;
    - *Subsystem*: *database* o *middleware;*

- *Network Monitoring*: servizio mirato all'interrogazione (*ping*, get SNMP, ecc.) e raccolta di segnalazioni (*trap*) da dispositivi di rete;
- HW *Monitoring*: servizio mirato all'interrogazione (*get* SNMP) e raccolta di segnalazioni (*trap*) dai *server* fisici;
- *Storage Monitoring*: servizio mirato all'interrogazione e raccolta di segnalazioni (*trap*) da dispositivi *storage* o *tool* di *performance*.

L'Offerente propone il seguente Sistema di Monitoraggio degli eventi infrastrutturali:

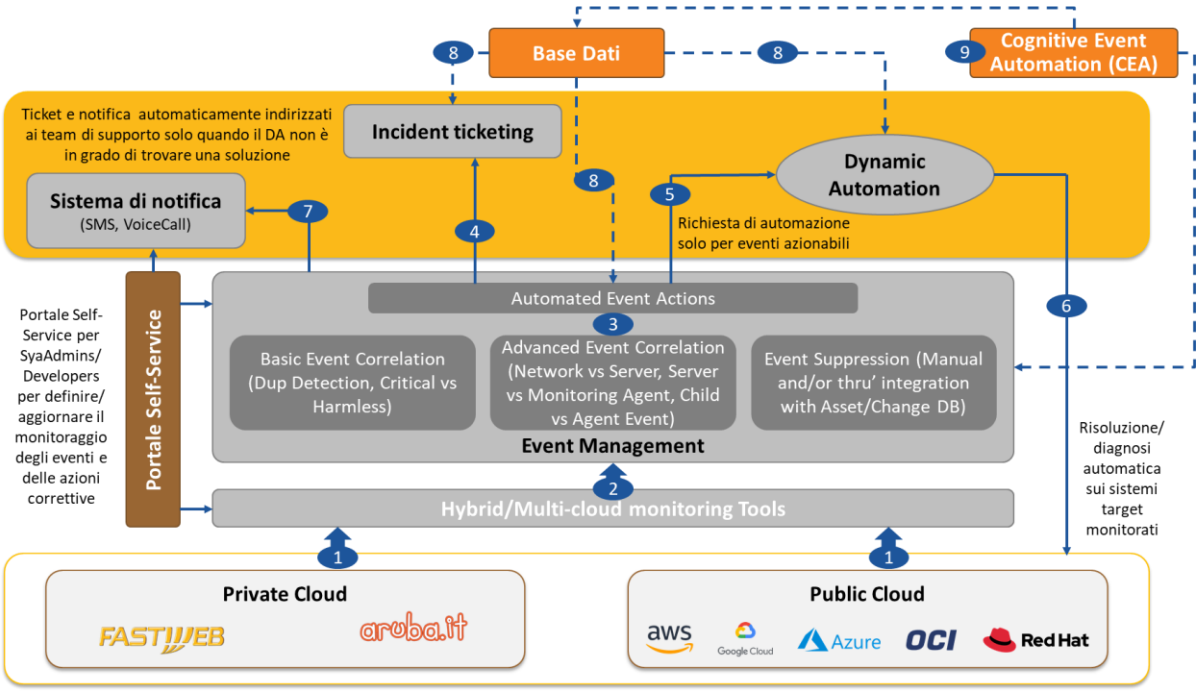



*Figura 14: Sistema di monitoraggio degli eventi infrastrutturali*

Il sistema di monitoraggio è direttamente integrato con la soluzione di *Event Management* che attraverso le attività di cattura, filtraggio, correlazione, interpretazione, soluzione e chiusura, supporta i processi di *Event*, *Problem*, *Availability*, *Capacity* e *Performance Management*.
Attraverso tale soluzione è possibile organizzare attività di monitoraggio su più livelli (*on site* e *off site*).
Il flusso del processo di *Event Management* si può schematizzare come segue:

1 gli agenti di monitoraggio inviano l'evento al *Server* di monitoraggio;
2 il *Server* convalida la correttezza del monitoraggio e inoltra gli eventi al Sistema di *Event Management;*
3 il Sistema di *Event Management* esegue la correlazione di base, inclusa la soppressione dell'evento se configurata, e la correlazione avanzata, identificando in tal modo gli eventi "*utilizzabili*";
4 il Sistema di *Event Management* crea *l'incident Ticket* (coda di automazione) per gli eventi utilizzabili;
5 il Sistema di *Event Management* invia, inoltre, una richiesta di automazione alla soluzione di *Automation;*
6 l'automazione dinamica esegue la diagnosi e l'eventuale riparazione dei sistemi gestiti;
7 se l'automazione dinamica non è in grado di risolvere il problema, l'evento viene profilato ed il sistema di *Event Management* apre il *ticket* e invia notifica al *team* di supporto;

8 la base dati estrae le informazioni dalle fonti sottostanti ed esegue analisi su:
   - Dati dell'evento dal Sistema di *Event Management;*
   - Dati di ticketing dal Sistema di *Ticketing* per *incident*;
   - Dati di automazione della soluzione di *Automation*.

9 il modulo *Cognitive Event Automation* (CEA) identifica le relazioni padre-figlio e gli eventi stagionali, alimentando il Sistema di *Event Management*.

#### *1.9.1.2 Event Log management*

Il servizio di "*Event Log Management*" ha lo scopo primario di tracciatura, conservazione ed analisi dei *log* generati dai componenti infrastrutturali e dalle piattaforme *cloud*, per costruire ed alimentare una base dati che può essere soggetta a successiva analisi, effettuando la caratterizzazione dei dati per migliorare il sistema di *Event Management*.
I sistemi operativi ed il *middleware* saranno in generale configurati secondo *i default* ai fini della tracciatura degli eventi e della scrittura dei *log*; i *log* saranno conservati in linea o sui sistemi di archiviazione per un periodo concordato con la PA utente (tipicamente da 1 a 3 mesi). Verranno utilizzati applicativi di *Log Collection* per sgravare da questo compito i sistemi ed avere una piattaforma centralizzata per il *Log Management* (es. *Logstash*).
Si prevede che i *log* di Sicurezza e quelli dettati da normative (quali ad esempio quella del Garante riguardo la protezione dei dati per gli amministratori di sistema) siano raccolti, e conservati sul sistema di *Log management* di responsabilità dell'Offerente.

### 1.9.2 Trouble Management

#### *1.9.2.1 Principali profili professionali coinvolti nel Trouble Management:*

- *Service Manager*: professionista responsabile di definire il servizio, gestire gli accordi sul livello dello stesso (*service level agreement*) ed assicurare che i servizi soddisfino le esigenze di *business*. Gestisce i membri del *team* del *service department*, valuta ed analizza le attività svolte, propone miglioramenti ai processi, inclusa l'interazione col *customer service* (reclami e richieste).
- *Service Delivery Manager*: professionista che si occupa di facilitare la produzione tempestiva di soluzioni gestendo in modo efficace i membri del *team*, il *budget* e gli orari di lavoro. Il suo ruolo si rivela fondamentale per eliminare eventuali ostacoli che possono rallentare il lavoro del *team*, incidendo negativamente sulla consegna delle soluzioni e sul rispetto delle scadenze.
- Operatore: professionista che si occupa della raccolta dei *ticket* di richieste di servizio, *change* e riparazioni di *incident* e di direzionarli verso i corretti *team* operativi. L'Operatore è responsabile, inoltre, della comunicazione verso il *Service Owner* ed altri soggetti interessati al servizio.
- *Service Owner*: professionista di riferimento lato PA utente per tutti gli aspetti tecnici e organizzativi che coinvolgono servizi ed esigenze di *business* presenti e future in carico alla NewCo.

#### *1.9.2.2 Gestione degli incident e dei problem*

A supporto della gestione degli *incident* e dei *problem* sono messi a disposizione una serie di strumenti e di procedure concordate con la PA utente, con lo scopo di avere il controllo completo del servizio che va dalla segnalazione, alla classificazione, fino alla risoluzione e chiusura *dell'incident/problem*.
*Incident* e *Problem Management* sono due processi strettamente correlati tra di loro nell'attività di gestione delle anomalie che si possono verificare durante l'erogazione dei servizi.

Il processo di *Incident Management* definisce le modalità di intervento a fronte del verificarsi di quegli eventi che, esulando dalla normalità, possono incidere sulla corretta esecuzione e sulla qualità dei servizi erogati. L'obiettivo primario consiste nel ripristino della disponibilità e del funzionamento atteso del servizio nel minor tempo possibile e con il minimo impatto, tramite soluzioni permanenti o temporanee (*workaround*) sul livello infrastrutturale.
Le azioni che scatenano tale processo possono essere attivate dagli utenti che sperimentano un malfunzionamento o dagli strumenti automatici di monitoraggio. Nella gestione *dell'Incident Management* ricadono le seguenti entità/richieste:

- incidenti;
- richieste di servizi (*Service Request*);
- richieste di modifica (*Change Request*).

Le fasi che identificano la gestione delle entità/richieste sono:

- identificazione e registrazione;
- classificazione e supporto iniziale;
- investigazione e diagnosi;
- risoluzione e ripristino;
- chiusura.

Le fasi precedentemente descritte sono riassunte nel seguente schema:

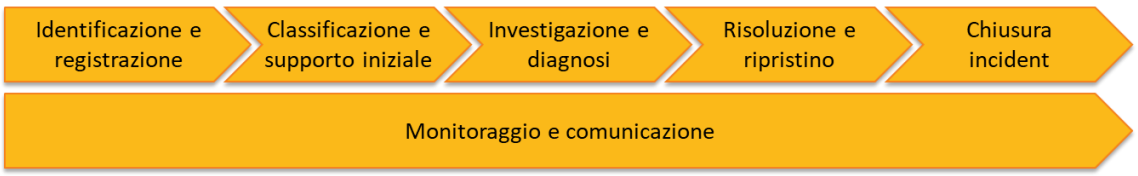



*Figura 15: Fasi di Incident Management*

Di seguito, vengono descritte le fasi del processo ITIL, riferimento per la definizione della procedura:

- identificazione: può essere effettuata sia dall'Operatore di *Service Desk* di livello 1 che riceve la chiamata dall'utente, sia automaticamente a seguito di un evento. La registrazione della chiamata avviene attraverso un ticket di *incident* nel sistema di IT *Service Management* (ITSM);
- classificazione: l'Operatore classifica l'evento e lo gestisce secondo competenza, assegnandolo alla coda opportuna. Se *l'incident* è aperto automaticamente da un evento, è direttamente assegnato alla coda di livello 2 che deve prenderlo in carico;
- investigazione e diagnosi: il livello 2 esegue una serie di passi diagnostici per l'analisi *dell'Incident* e, se necessario, si interfaccia con il *Service Owner*;
- risoluzione e ripristino: sulla base dell'analisi effettuata viene individuata una soluzione definitiva o temporanea; laddove non sia disponibile né l'una, né l'altra, *l'incident* viene incanalato nel flusso di processo di *Problem Management*;
    - se la risoluzione è di competenza del *Service Desk* di livello 1, *l'incident ticket* viene inviato all'Operatore per la conferma di chiusura e comunicazione con l'utente;
    - se la risoluzione è di competenza dei *team* specialistici di livello 2, il gruppo specifico la gestisce direttamente;
    - per gli *incident* proattivi aperti automaticamente (ad esempio, un *warning* inerente ad uno spazio che si sta esaurendo), la risoluzione e il ripristino non passano dal *Service Desk* di livello 1, ma vengono gestiti dal livello 2 in autonomia, oppure viene coinvolto *l'account team*, nel caso in cui sia necessario

invocare altri processi (per esempio, se il *warning* proattivo implica l'analisi sulla *capacity,* o la gestione della *demand* con il coinvolgimento della PA utente);

- monitoraggio: il *Service Delivery Manager* esegue una valutazione dei *task* effettuati e rivede il processo. Il Monitoraggio permette di stabilire se la risoluzione dell'*incident* ha avuto esito positivo e se è stata effettuata nel rispetto dei livelli di servizio accordati. Al termine della valutazione viene generato un *report* che tiene traccia dell'andamento del processo.

Il processo di Problem Management si occupa di individuare la causa alla base di un evento significativo per cui non è ancora disponibile una soluzione.
Le fasi in cui si articola il processo di *Problem Management* sono:

- identificazione e registrazione evento;
- classificazione;
- investigazione e diagnosi;
- identificazione e registrazione dell'errore;
- analisi dell'errore;
- registrazione e risoluzione dell'errore nel *Known Error* DB;
- chiusura evento (in caso di *problem* o errore noto che non sia correttamente identificato in fase di analisi *dell'incident*).

Le fasi precedentemente descritte sono riassunte nel seguente schema:




*Figura 16: Fasi del Problem Management*

I processi di *Incident* e *Problem Management* sono strettamente correlati; in particolare:

- l'*Incident Management* invoca il *Problem Management* qualora:
  - nel corso della fase investigativa *dell'incident* non sia stata trovata una soluzione nota;
  - si voglia richiedere un'ulteriore *Root Cause Analysis;*
  - si voglia comunicare la soluzione determinata durante le fasi di investigazione e risoluzione;
- il *Problem Management* invoca *l'Incident Management* quando:
  - si voglia comunicare la risoluzione di un problema e degli incidenti associati;
  - si voglia comunicare l'esistenza di un nuovo errore e di una soluzione per risolverlo.

Entrambi i processi sono contraddistinti da un'attività di controllo e comunicazione comune e prevedono l'interazione con le entità del *Change* e *Configuration Management*.
L'interazione con le altre entità è evidenziata nei due schemi successivi:

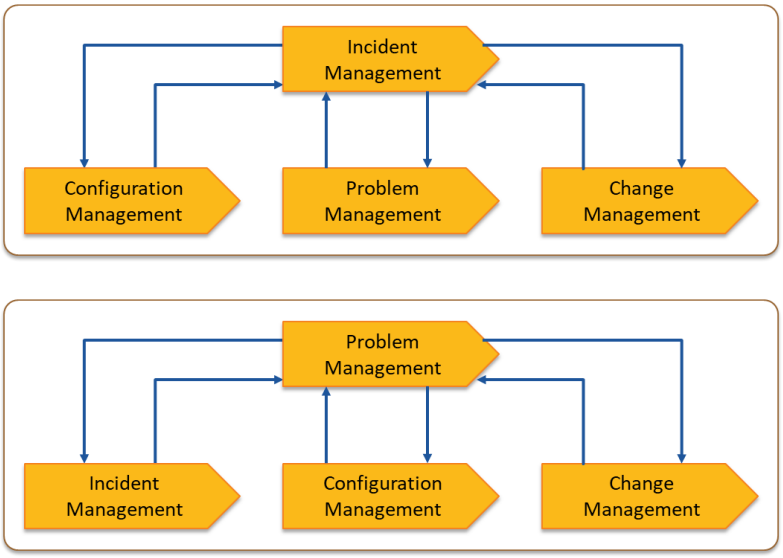



*Figura 17: Interazione tra Incident e Problem Management*

I processi di *Incident* e *Problem Management* sono governati da un'organizzazione fondata su figure di riferimento con compiti definiti per ottimizzare i tempi di intervento e per raggiungere l'efficacia/l'efficienza dell'intervento stesso.
La gestione di *Incident* e *Problem* è supportata dall'apposito modulo del Sistema di ITSM, che fornisce le funzionalità necessarie ad una gestione completa dei *Ticket* (per entrambi i processi) ed opera in modalità integrata con le altre applicazioni di ITSM (*Change*, *Asset* e *Configuration*).
Le principali funzionalità permettono:

- l'apertura del *Ticket* (anche utilizzando modelli predefiniti), la sua classificazione, la registrazione del disservizio rilevato dall'utente, la definizione dell'impatto, dell'urgenza e della priorità, l'eventuale assegnazione ai gruppi di assistenza;
- la gestione completa del ciclo di vita del *Ticket* fino alla sua chiusura;
- Il controllo dell'accesso ai *Ticket* in base al loro stato ed al ruolo del tecnico, ad esempio per permettere solo ad un gruppo di tecnici la chiusura del *Ticket* stesso;
- il controllo del Livello di Servizio del singolo *Ticket*, in modo da poter operare conformemente al Livello di Servizio richiesto;
- l'invio di notifiche, ove opportuno;
- la ricerca di soluzioni conosciute rispetto al disservizio segnalato, mediante l'integrazione con il modulo di *Knowledge Management* del sistema di ITSM;
- la gestione di *Incident* pervasivi;
- le funzionalità di integrazione con altre applicazioni (ad esempio, l'apertura automatica di un *incident* a fronte di un evento notificato dal sistema di monitoraggio).

Grazie all'integrazione con l'anagrafica utente e *l'asset management*, ogni *Ticket* include le informazioni dell'utente, dell'*asset* impattato e delle loro localizzazioni di riferimento, senza che l'operatore le debba inserire manualmente.
Mediante l'integrazione con il modulo di *Knowledge Management* dell'ITSM, gli operatori di *Service Desk* e i tecnici dei gruppi di supporto sono in grado di cercare soluzioni conosciute al problema segnalato; qualora una soluzione venga trovata ed applicata con successo il sistema aggiorna automaticamente il *Ticket* con la descrizione trovata nell'articolo senza che l'operatore debba farlo manualmente.
Nel sistema sono, inoltre, presenti specifici modelli (*Template*), utilizzabili per le segnalazioni più frequenti, mediante i quali gli operatori possono compilare rapidamente il *Ticket*,

mantenendo un elevato livello qualitativo grazie alla presenza di campi precompilati con parametri e testi predefiniti in fase di disegno del modello stesso.
Un aspetto importante è la capacità di gestione degli *Incident* di tipo pervasivo; per questo il sistema permette di mettere in relazione tra loro diversi *Ticket* (altri *Incident*, *Change*, Richieste di servizio, *Problem*) in modo da ricondurli alla medesima causa e facilitarne la gestione aggregata (es. la risoluzione *dell'Incident* pervasivo "o *Ticket* padre" risolve tutti i *Ticket* di *Incident* ad esso correlati o "*Ticket* figli") permettendo, quindi, una gestione più agevole e riducendo drasticamente i margini di errore nel loro aggiornamento.
Particolare attenzione è prestata, inoltre, alle informazioni per la misurazione dei livelli di servizio associati al singolo *Ticket*, calcolati considerando gli orari di servizio ed il calendario delle festività.
Il processo dell'Offerente, e la relativa configurazione del Servizio di ITSM, prevede di categorizzare la priorità degli *Incident* secondo la matrice "impatto/criticità". Di seguito se ne riporta la descrizione:

- criticità: la criticità degli *asset* IT infrastrutturali sarà stabilita durante il periodo di transizione e trasformazione in base alle informazioni fornite dalla PA utente (es. le applicazioni, i processi di *business*, l'architettura infrastrutturale), ed a seconda della mappatura tra applicativi e componenti infrastrutturali;
    - in particolare, si definisce '*Funzione Critica*' un sistema o un'applicazione che la PA utente abbia identificato in forma scritta e comunicato precedentemente alla NewCo come fortemente impattante del proprio *business*; per tali tipologie di funzioni, è necessario definire un adeguato piano di ripristino del servizio che sia in grado di ristabilire i *target* operativi attesi, nelle tempistiche desiderate (nessun *single point of failure*);
    - tale classificazione potrà essere rivista periodicamente o in presenza di situazioni che possono influenzare la criticità degli *asset*. Variazioni significative delle criticità degli *asset* IT infrastrutturali potranno dare origine a variazioni dei Servizi secondo il processo di *Change Management*;
    - i livelli di criticità sono: alta, media, bassa.
- impatto: il livello di impatto di un *Incident* sul *business* della PA utente e dei destinatari dei servizi è categorizzato come segue:

*Tabella 1: Categorizzazione del livello di impatto di un incident*

| Livello di impatto | Definizione |
|---|---|
| Critico | • L'infrastruttura a supporto di un'applicazione o processo di *business* è completamente indisponibile, con possibili evidenti impatti economici e/o reputazionali e/o normativi per il Cliente e/o pervasività su più di un Destinatario dei Servizi;<br>• Un servizio *core/trasversale* di *cloud*/DC è totalmente indisponibile (e.g. *network*, *firewall*, *storage*, accesso ai mercati, accesso ad *Internet*) per più di un Destinatario dei Servizi |
| Alto | • L'infrastruttura a supporto di una applicazione o processo di *business* è completamente indisponibile per un solo Destinatario dei Servizi, con il risultato di bloccare un processo di *business*<br>• Un servizio *core/trasversale* di *cloud*/DC è parzialmente indisponibile (e.g. *network*, *firewall*, *storage*, accesso ai mercati, accesso ad *Internet*) per uno o più di un Destinatario dei Servizi |
| Medio | • L'infrastruttura a supporto di un'applicazione o di un processo di *business* è parzialmente indisponibile, così come avvertito da un gruppo significativo di utenti finali (almeno 10) |

| | |
|---|---|
| Basso | • *Incident* che non rientra nelle categorie precedenti |

La priorità degli *incident* verrà calcolata per i Servizi di *cloud*/DC come prodotto della criticità degli asset IT infrastrutturali (Alta, Media, Bassa) e del Livello di Impatto (Critico, Alto, Medio, Basso).

*Tabella 2: Definizione priorità degli Incident*

| Livello di impatto | Criticità IT asset | | |
|---|---|---|---|
| | Alta | Media | Bassa |
| Critico | P1 | P2 | P2 |
| Alto | P2 | P2 | P3 |
| Medio | P3 | P3 | P3 |
| Basso | P3 | P3 | P3 |

Di seguito si riportano i livelli di servizio offerti a seconda dei diversi gradi di prioritizzazione degli *Incident*:

*Tabella 3: Livelli di servizio offerti dall'Offerente*

| Priorità | Descrizione | Tempo max di risoluzione |
|---|---|---|
| Priorità 1 | • Una funzione critica o un disservizio infrastrutturale che causa grandi impatti al servizio (*High Impact*) e non è disponibile una soluzione alternativa | <= 2 ore |
| Priorità 2 | • Presenza di un impatto potenzialmente elevato o un servizio relativo ad una funzione critica degradata e contemporanea mancanza di soluzione alternativa<br>• Disservizio su una funzione non critica che causa un impatto medio al *business* della PA senza soluzione alternativa. Tutte le componenti dei sistemi devono essere in alta affidabilità | <= 4 ore |
| Priorità 3 | • Indisponibilità o inutilizzabilità di una funzione non critica che causi impatti medi/bassi alla PA utente, ma senza un impatto immediato e rilevante sul *business* del Cliente e senza che sia disponibile una soluzione alternativa<br>• Gli incidenti P1 e P2 per cui sia applicabile un *bypass* o un'alternativa accettabile per la risoluzione *dell'incident* verranno riclassificati come P3 | <= 6 ore |

### 1.9.3 Tracciamento dei ticket

Le soluzioni dell'Offerente nell'area del *service management* permettono l'evoluzione delle *Operation* IT verso un modello proattivo e predittivo. L'Offerente propone l'utilizzo di una soluzione di *Automation* che permetta di raccogliere dati da diverse fonti, quali *log file*, eventi, metriche di *performance* e *ticket*, di esaminarle in un contesto più ampio e di supportare l'identificazione proattiva dei problemi prima della loro occorrenza.
Tale soluzione include infatti **funzionalità di *Analytics* e *Machine Learning-cognitive***, che permettono di raggiungere nuovi livelli di automazione intelligente. Gli elementi di automazione tradizionale già sviluppati vengono integrati e riutilizzati in un *framework* più ampio in grado di decidere in tempo reale le modalità di intervento e di replicare in maniera robotica una tipica interfaccia umana integrando diversi sistemi ed applicazioni; ne deriva **una riduzione del volume degli *incident* e del tempo medio di risoluzione** (MTTR).
La soluzione di *Automation* si applica in ambito *server*, *database* e *middleware*.
Nella figura seguente si illustra una sintesi dei risultati ottenibili dall'implementazione della soluzione di *Automation*:




*Figura 18: Risultati della soluzione di Automation*

La soluzione di *Automation* svolge cinque attività, divise in tre raggruppamenti logici:

- **attività di raccolta** (*activity collation*): attività da eseguire sui vari sistemi per il supporto dei processi di *Trouble Management*. Queste attività potrebbero riguardare: eventi dei sistemi di monitoraggio dei *server*, richieste di servizio, ordini di lavoro di altri sistemi (ad es. Servizio di ITSM *Service Catalog*), etc.
- **riduzione delle attività** (*activity reduction*): riconciliazione degli eventi per ricondursi a quelli che necessitano di risoluzione. I sistemi di gestione degli eventi, infatti, sono diventati funzionalmente più ricchi ed eseguono una correlazione automatizzata degli eventi (sfruttando le informazioni sulla tipologia o applicando la correlazione attraverso l'analisi avanzata degli eventi).
- **esecuzione dell'automazione** (*automation execution*): una volta stabiliti i flussi di attività necessari e sufficienti, si applicano diversi livelli di automazione a seconda del tipo di problematica e investigazione di interesse. Le automazioni possono essere eseguite su sistemi *target* o possono includere attività a livello di altri sistemi di gestione.
- **rilevamento delle attività** (*activity tracking*): il sistema di *incident*, *problem* e *change management* mantiene informazioni dettagliate su tutte le attività che si svolgono durante il ciclo di vita dell'automazione. Gli stessi *ticket* possono anche essere necessari per il completamento o la risoluzione da parte di un essere umano in caso di insuccesso da parte dell'automazione; potrebbero anche successivamente essere utilizzati nell'ambito della *Root Cause Analysis*.

- misurazioni, documentazione ed analisi (*measurement*, *reporting* and *analytics*): le analisi condotte in questa fase sono funzionali al miglioramento continuo della soluzione di automazione (ad esempio: quali eventi filtrare, cosa automatizzare in seguito, ecc.).

Lo schema di una possibile soluzione di *Automation* è illustrato di seguito:

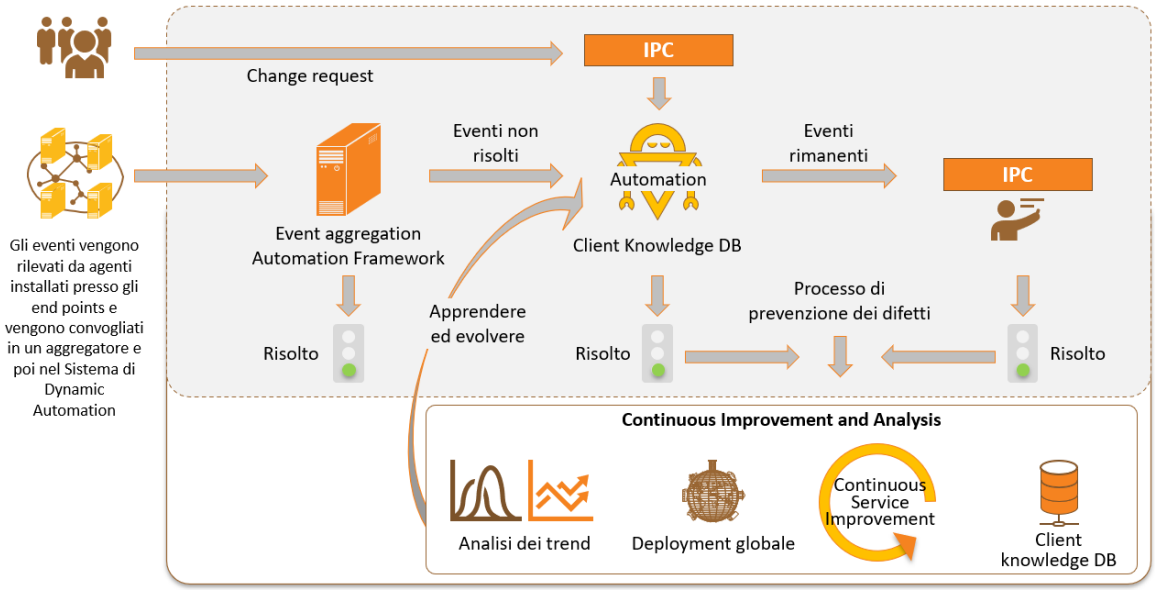



*Figura 19: Soluzione di Automation (Incident, Problem, Change Management)*

Gli agenti di monitoraggio del sistema, installati presso gli *end point* inviano un avviso al superamento di soglie prestabilite. Gli avvisi verranno consolidati in un aggregatore di eventi.
Le regole di automazione esistenti vengono implementate per eseguire la correlazione degli eventi atta ad eliminare i duplicati.
Attraverso un bridge automatico con la piattaforma di *Event Management*, un ingegnere virtuale lancerà un *playbook* sviluppato per l'evento specifico. In caso di successo, verrà utilizzato un bridge automatizzato con il sistema ITSM per aprire un *incident* e contrassegnarlo come risolto.
Se l'automazione non sarà in grado di risolvere l'evento, lo stesso *bridge* aprirà un *ticket* di *incident* e lo inoltrerà ad un Operatore per la corretta gestione.
Quando un ingegnere virtuale inoltra un *incident* ad un Operatore, compie due passaggi cruciali:

- registra tutti i dettagli per popolare *l'incident ticket* con tutti gli elementi avanzati per la risoluzione;
- contrassegna come fallita l'auto-risoluzione.

Queste informazioni servono come *input* per il processo di continuo miglioramento. I dati raccolti dalla soluzione di *Automation* vengono infatti inviati alla piattaforma di analisi e reportistica.
Tale piattaforma fornisce informazioni utili all'ottimizzazione del servizio, basate su relazioni tra una vasta gamma di dati provenienti dagli strumenti utilizzati per la gestione delle risorse IT. Queste informazioni sono aggregate in analisi retrospettive, *dashboard* attuali (incluse *dashboard* in tempo reale), raccomandazioni future per efficientare il servizio ed approfondimenti predittivi per ridurre gli *incident* o migliorare la gestione di *change*, basati sull'analisi cognitiva dei dati. Gli esiti disponibili coprono molti dei principali domini di servizio

(per esempio, *Change*, *Incident* e *Capacity*) con un'enfasi particolare su *Incident* and *Automation Insights*, e sono utilizzati per alimentare la *Console* del sistema di *Automation*, a supporto di investigazioni e risoluzioni future.

### *1.9.4 Configuration management Data Base*

Obiettivo del servizio è assicurare l'identificazione, il controllo e la manutenzione delle versioni di tutti gli elementi di configurazione relativi alle componenti IT (e.g. *hardware*, *software* di base e documentazione correlata), comprensive delle relazioni tra le stesse in ottica *end-to-end*, garantendone l'aggiornamento in seguito ad interventi di manutenzione, all'implementazione di nuove soluzioni o nuovi servizi. La NewCo definirà un *Configuration Management DataBase* (CMDB), utilizzando le migliori tecnologie di mercato, dove verranno inserite tutte le componenti infrastrutturali (*configuration* item) ed i legami esistenti tra queste. Alla presa in carico del servizio, e durante il periodo di migrazione, la NewCo effettuerà un censimento di tutti gli *asset* tecnologici tramite l'analisi della documentazione disponibile e la scansione di tutte le reti attualmente in uso mediante strumenti di *discovery*.
Al fine di mantenere realmente efficace nel tempo la soluzione CMDB/ *Configuration Management* si prevede di eseguire i seguenti processi secondo gli standard ITIL, che coinvolgono tutti gli elementi della configurazione:

1 identificazione: definisce i tipi di elementi della configurazione e gli attributi che verranno posti sotto il controllo del *Configuration Management*;
2 controllo: assicura che tutte le aggiunte, gli aggiornamenti e le eliminazioni dispongano della documentazione di controllo appropriata;
3 *report*: assicura che le informazioni per tutti gli elementi di configurazione siano disponibili per qualsiasi richiedente autorizzato;
4 verifica ed a*udit*: verifica che il CMDB rifletta accuratamente l'ambiente e gli *standard* stabiliti eseguendo *audit* periodici seguiti da un processo di riparazione per correggere eventuali discrepanze.

#### *1.9.4.1 Asset discovery*

La NewCo prevede la gestione ed implementazione delle attività e delle funzionalità automatizzate di *Asset Discovery*. *L'Asset Discovery* è indispensabile per mantenere l'integrità e la completezza delle informazioni nel CMDB; essa supporta, inoltre, la possibilità di registrare nel CMDB le relazioni e le dipendenze tra *server*, *middleware* e *database* e il popolamento di attributi che sarebbe inefficiente raccogliere a mano. Consente, infine, di implementare dei controlli sulle differenze tra quanto registrato nel CMDB e quanto rilevato dalla *discovery* stessa. L'attività di *discovery* automatica eseguita dagli strumenti predisposti dalla NewCo viene arricchita dal contributo di personale specializzato con il compito di inserire nel CMDB le informazioni di *service management* che non è possibile raccogliere in automatico dai sistemi, ma che supportano gli altri processi collegati al *Configuration Management*. A titolo di esempio, si cita lo SLA, usato dal processo di *incident*, ma anche, eventualmente, la consuntivazione degli *asset*.

*Tabella 4: CMDB – Asset discovery*

| Area | Descrizione |
|---|---|
| *Incident management* | I *Configuration Item* che rappresentano i sistemi dell'ambiente IT sono collegati agli *incident* appropriati |
| *Change management* | Uno o più *Configuration Item* sono collegati ad ogni richiesta di *change*, fornendo così uno storico dei *change* che può aiutare nell'analisi degli *incident* |

| | |
|---|---|
| *Asset management* | I *Configuration Item* sono collegati ai dati di *asset* e questo allineamento è verificato nella reportistica ed *auditing* sulla qualità dei dati |
| *Service request* | I *Configuration Item* possono essere collegati alle *Service Request* per fornire ulteriori dettagli tecnici sulla richiesta |

### 1.9.5 Cartografia *hardware* e *software*

Nei paragrafi precedenti è stato descritto il CMDB nella sua funzione principale, ma anche nel meccanismo di aggiornamento continuo, finalizzato alla disponibilità di dati sempre aggiornati e corretti.
Ovviamente, l'adozione degli strumenti costituisce una base, ma la parte rimanente delle attività deve essere svolta attraverso i processi, ad esempio *l'asset management*, che fornisce le informazioni relative alla "creazione" del componente *hardware* e ne certifica la "cancellazione". Tali informazioni arricchiscono le funzionalità disponibili con la soluzione di *asset discovery* precedentemente descritta e ne costituiscono un punto di controllo, rendendo possibile gestire l'intero ciclo di vita delle componenti *Hardware* e *Software* per tipologia e condizione di utilizzo nell'ambito del servizio, integrando informazioni aggiuntive ove necessario.

## 1.10 ID CRITERIO:10 – TABELLARE – RIDUZIONE SUL PERIODO MINIMO DI DISPONIBILITÀ DELL'INFRASTRUTTURA DI 180 GIORNI. IL CRONOPROGRAMMA DOVRÀ EVIDENZIARE TUTTI GLI STEP RELATIVI ALLA DISPONIBILITÀ DELL'INFRASTRUTTURA EVIDENZIANDO LE PROPOSTE CHE PRESENTINO LA MAGGIOR CELERITÀ REALIZZATIVA.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|
| **10** | Tabellare | Disponilità | Parte migliorativa relativa alla riduzione dei tempi di disponibilità dell'infrastruttura (cfr. IQ07) | Riduzione sul periodo minimo di disponibilità dell'infrastruttura di 180 giorni. Il cronoprogramma dovrà evidenziare tutti gli step relativi alla disponibilità dell'infrastruttura evidenziando le proposte che presentino la maggior celerità realizzativa. | 0,1 punti ogni giorno di riduzione, fino ad un massimo di 60 giorni, sul periodo minimo di 180 giorni | **6** |

L'Offerente propone un netto miglioramento del periodo di disponibilità dell'infrastruttura - definita dall'Addendum come "*Polo Strategico Nazionale, di cui al comma 1 dell'articolo 33-septies del D.L. n. 179 del 2012, come esposto nel progetto di fattibilità allegato al presente disciplinare di gara*" -, portando il valore base previsto nel bando da 180 giorni a **120 giorni**, come sintetizzato nella tabella seguente:

Riduzione dei tempi di disponibilità dell'infrastruttura

| |
|---|
| Punteggio indirizzato dall'Offerente = 6 punti |

| | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: 180 giorni | Valore dell'Offerente: 120 giorni |

Il miglioramento è reso possibile grazie a diversi fattori che includono, fra gli altri, la disponibilità da subito di alcuni dei DC individuati per il PSN e degli elementi principali dell'infrastruttura - come la rete per il collegamento dei DC e della maggior parte delle PA utenti, le competenze e i servizi già disponibili in ambito *cloud*, gli accordi pregressi con i CSP, la parallelizzazione di diverse attività nel cronoprogramma - che rendono possibile la migrazione delle Amministrazioni utenti e l'avvio dei servizi del PSN, a norma dell'art. 6, comma 2, della BdC. Per maggiore chiarezza, si intende per disponibilità dell'infrastruttura PSN, la messa a disposizione di tutti gli *asset* necessari per avviare la migrazione dei *server* delle PA e la prestazione dei servizi di base del PSN, ai sensi dell'art. 6, comma 2, della BdC. Tali *asset* sono costituiti da: disponibilità dei DC e relativa connessione, in grado di erogare i servizi di migrazione e i servizi *cloud* di base (es. *Housing, Hosting, Iaas Private Cloud*).
Nelle seguenti sezioni sono presentati:

- il cronoprogramma di alto livello (il "Cronoprogramma") e le principali *milestone*;
- un diagramma di Gantt di maggior dettaglio, inclusa la descrizione delle attività principali ivi rappresentate.

### 1.10.1 Cronoprogramma di alto livello e *milestone*

Il Cronoprogramma è strutturato in diversi filoni progettuali ("*stream*"), con un elevato livello di parallelismo, per garantire la riduzione dei tempi di disponibilità dell'infrastruttura. Opportune contromisure saranno adottate per il contenimento dei rischi di ritardo e realizzazione, come descritto in seguito (cfr. 1.10.2).

Nella figura sottostante è riportato il Cronoprogramma, con partenza alla data di sottoscrizione della Convenzione ("T0") fino al momento di disponibilità dell'infrastruttura.
Le società che costituiscono l'Offerente, in qualità di primari operatori di servizi *cloud,* hanno già attivi degli importanti piani di investimento infrastrutturali che includono diverse delle tecnologie pensate per il PSN.
Ne consegue che alcune delle componenti di infrastruttura e servizio, propedeutiche al PSN, saranno già disponibili al momento T0, rendendo così possibile una compressione dei tempi.

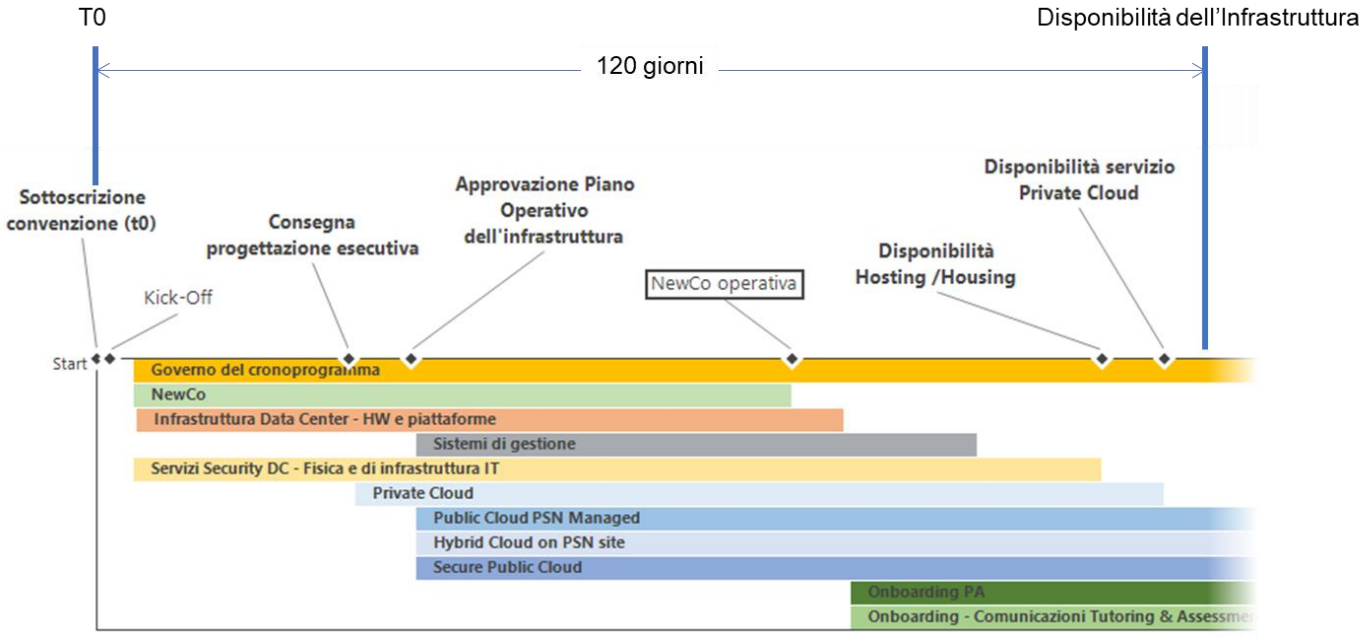



*Figura 20: Cronoprogramma*

Gli *stream* previsti sono:

1. Governo del Cronoprogramma
   a. Include tutte le attività necessarie alla pianificazione, controllo e conduzione del Cronoprogramma, dal momento della sottoscrizione della convenzione fino alle fasi di Verifica di Conformità;
2. NewCo
   a. Include tutte le attività necessarie alla costituzione della NewCo, ed altri aspetti societari;
3. Infrastruttura DC
   a. Relativa alla progettazione e realizzazione dell'infrastruttura dei DC, inclusa la loro interconnessione;
4. *Security*
   a. Inerente alla realizzazione di tutti gli aspetti legati alla sicurezza del PSN. Nel Cronoprogramma sono rappresentate solo le attività necessarie alla disponibilità dell'Infrastruttura. Lo *stream* proseguirà anche dopo la data di disponibilità dell'Infrastruttura (non rappresentato nel Cronoprogramma e nel Gantt), in particolare per tutto ciò che riguarda i servizi *Public Cloud* con i CSP;
5. *Private Cloud*
   a. Inerente alle attività per la progettazione e messa in opera dei servizi *Private Cloud*;
6. *Public Cloud* PSN *Managed*
   a. Inerente alle attività per la progettazione e messa in opera dei servizi *Public Cloud* PSN *Managed,* che saranno avviate nella finestra temporale del Cronoprogramma ma termineranno a valle della Disponibilità dell'Infrastruttura;
7. *Secure Public Cloud*
   a. Inerente alle attività per la progettazione e messa in opera dei servizi *Secure Public Cloud,* che saranno avviate nella finestra temporale del Cronoprogramma ma termineranno a valle della Disponibilità dell'Infrastruttura;

8. *Hybrid Cloud on PSN Site*
    a. Inerente alle attività per la progettazione e messa in opera de servizi *Hybrid Cloud*, che saranno avviate nella finestra temporale del Cronoprogramma ma termineranno a valle della Disponibilità dell'Infrastruttura;
9. *On boarding* PA
    a. Relativo alle attività di comunicazione e ingaggio delle PA utenti ai servizi del PSN.

Di seguito si riportano le principali *milestone* del Cronoprogramma:

*Tabella 5: Milestone del Cronoprogramma*

| Milestone | Tempo | Descrizione |
|---|---|---|
| Firma della Concessione | T0 | Avvio del Cronoprogramma |
| Nomine NewCo | T0 + 20 giorni | Nomine, ai sensi dell'Art 13 della BdC, e comunicazione al MITD |
| Disponibilità del Piano Operativo dell'infrastruttura e invio al MITD | T0 + 30 giorni | Disponibilità del Piano Operativo dell'Infrastruttura ed invio per approvazione da parte del Concedente entro 30 giorni, ai sensi dell'Art 16 della BdC. |
| Newco Operativa | T0 + 75 giorni | Conclusione delle attività necessarie per rendere la NewCo operativa. |
| Disponibilità infrastruttura | T0 + 120 giorni | Disponibilità dell'infrastruttura e comunicazione al MITD |

### 1.10.2 Gantt ed attività

Di seguito, è rappresentato il Gantt del Cronoprogramma, qui riportato in forma compressa per motivi di leggibilità.

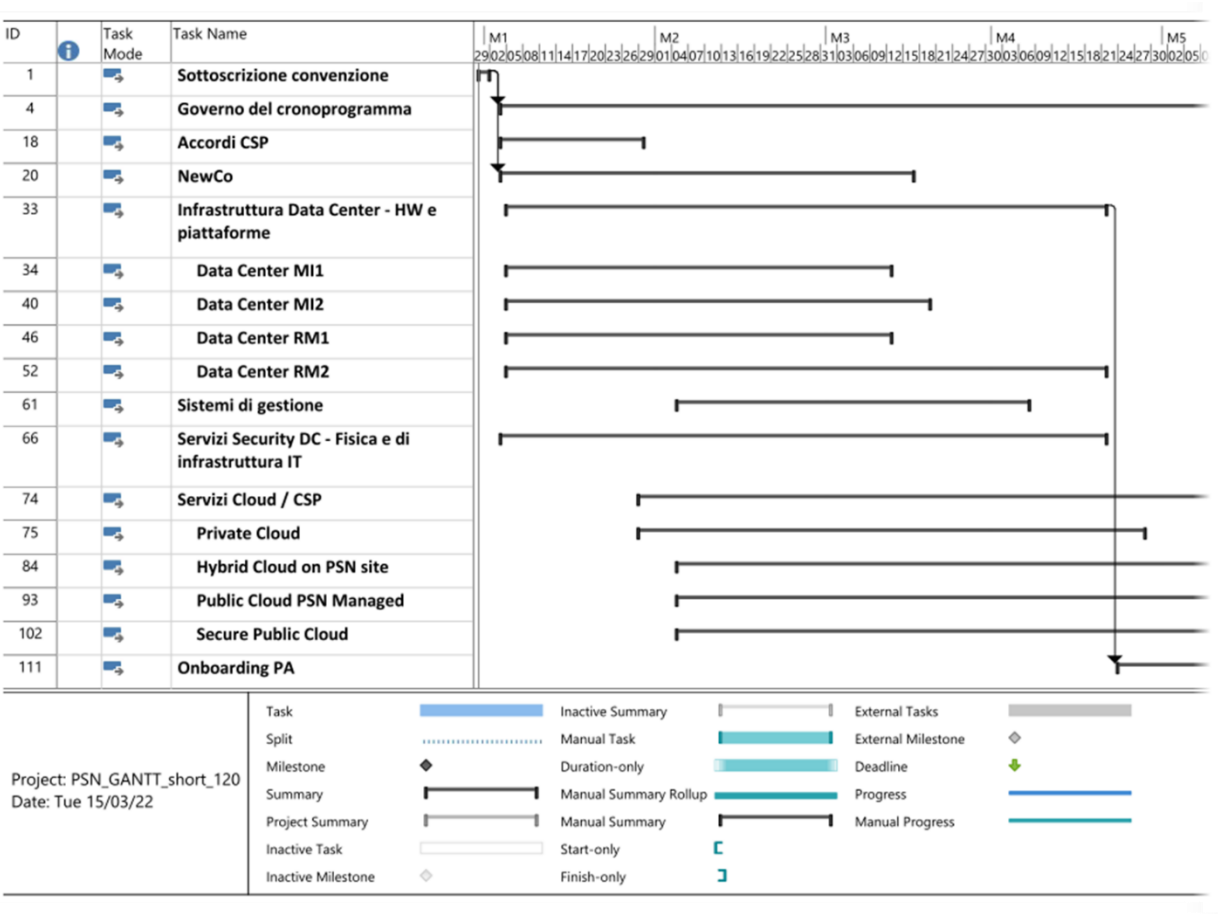



*Figura 21: Gantt*

Nella tabella seguente è riportata la descrizione delle attività del Gantt. **Sono riportate solo le attività rilevanti nella finestra temporale che va dalla firma della Concessione alla Disponibilità dell'Infrastruttura.**

*Tabella 6: Descrizione attività del Gantt*

| Stream | Attività | Descrizione |
|---|---|---|
| Governo del Cronoprogramma – Principali attività | | |
| Governo del Cronoprogramma | Cabina di regia e controllo | Include la costituzione di una **cabina di regia** e **l'esecuzione** di tutte le attività necessarie al **governo del Cronoprogramma**, inclusa la adozione di opportune azioni di ***contingency*** **che si dovessero rendere necessarie per il rispetto dei tempi previsti**.<br><br>Le azioni di *contingency* si dividono in due categorie principali:<br>• *Workforce* ed extra *effort* in termini di numero di persone ed estensione degli orari di lavoro nel caso debba essere attivato un *recovery plan* per il recupero |

| Stream | Attività | Descrizione |
|---|---|---|
| | | di ritardi accumulati (sia per cause endogene che esogene);<br>• Maggiore parallelizzazione di attività disomogenee, che non hanno sovrapposizioni in termini di personale dedicato all'implementazione. |
| Governo del Cronoprogramma | Piano Operativo - Progettazione esecutiva e *test plan* per collaudo finale | Stesura del **Piano Operativo dell'infrastruttura**, per la componente di **progettazione**. Il **progetto esecutivo complessivo** sarà raccordato con i progetti di dettaglio delle singole componenti del PSN. La progettazione sarà effettuata nelle prime fasi del Cronoprogramma e potrà richiedere in corso d'opera degli affinamenti/variazioni che saranno opportunamente gestiti e recepiti nei documenti di progettazione.<br><br>Sarà, inoltre, definito in questa fase il **piano di *test* a supporto della fase di Verifica di Conformità** (da effettuarsi al momento del completamento dell'infrastruttura, ai sensi della BdC).<br>I piani di test "verticali" dei singoli *workstream* sono invece definiti all'interno degli stessi. |
| Governo del Cronoprogramma | Piano Operativo - Pianificazione e *Risk Management* | Stesura del **Piano Operativo dell'infrastruttura**, per le componenti di piano complessivo (***Master Plan***) e relativo piano di contenimento dei rischi (***Risk Management Plan***).<br>Il ***Master Plan*** sarà opportunamente raccordato con i diversi piani di dettaglio degli *stream* nel Cronoprogramma (es. infrastrutture, servizi *cloud*, etc.) |
| Accordi CSP – Principali attività | | |
| Accordi CSP | Conversione accordi attuali in accordi con la NewCo | Azioni necessarie alla conversione degli accordi in essere con i CSP, in **accordi tra la NewCo e i CSP**. |
| NewCo – Principali Attività | | |
| NewCo | Assunzione personale | **Assunzione del personale** della NewCo con le competenze necessarie alla corretta erogazione dei servizi del PSN, secondo i criteri definiti nella documentazione di gara e le migliorie proposte nell'Offerta. |
| NewCo | Disegno ed attuazione dell'organizzazione | Disegno di dettaglio e messa in esecuzione di tutti gli **aspetti organizzativi** necessari al PSN (ad es. unità organizzative, ruoli, processi e |

| Stream | Attività | Descrizione |
|---|---|---|
| | | strumenti), incluse le nomine previste dalla BdC. |
| NewCo | *Training* | **Formazione** del personale con l'obiettivo di rendere la NewCo completamente operativa al momento della Disponibilità dell'Infrastruttura. |
| Infrastruttura Data Center – Principali attività | | |
| Infrastruttura *Data Center – Hardware* e piattaforme piattaforme | Progettazione esecutiva dettagliata (LLD) | **Progettazione di dettaglio** dell'infrastruttura PSN, compresi i DC, le connessioni di rete e le interconnessioni e tutti gli altri elementi infrastrutturali previsti, raccordata con il Piano Operativo complessivo. |
| | Certificazioni | Ottenimento di eventuali ulteriori certificazioni necessarie per i DC. |
| | Disponibilità spazi | Predisposizione ed allestimento degli spazi nei DC al fine di abilitare le successive fasi operative. |
| | Connettività | Predisposizione dei collegamenti tra la *backbone* e i DC al fine di abilitare l'interconnessione tra i servizi resi disponibili. |
| | *Set-up* ambienti | Predisposizione degli ambienti sui quali saranno resi disponibili i servizi. |
| | Allestimento *rack* e cablaggi | Predisposizione delle sale in cui saranno installati i *server* attraverso l'allestimento dei *rack* e dei cablaggi necessari per garantire l'operatività. |
| | Collaudo Infrastruttura DC | Collaudi dell'infrastruttura. |
| Sistemi di Gestione – Principali attività | | |
| Sistemi di Gestione | Progettazione esecutiva | **Progettazione di dettaglio** degli sviluppi applicativi necessari ai sistemi di gestione previsti dall'Offerta. I sistemi di gestione includono, ad esempio: gli strumenti di *monitoring* e di *ticketing*, gli strumenti a supporto delle migrazioni, il portale di fornitura, gli strumenti di *reporting*, etc. |
| | Sviluppo *software* | **Sviluppi** *software*, come definiti in fase di progettazione esecutiva. |
| | *Test* e collaudi | Attività di *test* e collaudo sui sistemi di gestione.<br>Le attività saranno effettuate in modo da verificare in modo completo **l'adeguatezza a quanto previsto dal Bando di Gara e dall'Offerta** |

| Stream | Attività | Descrizione |
|---|---|---|
| | | di tali sistemi, in termini di, ad esempio, funzionalità, esercizio e *performance*. |
| Servizi *Security* DC – fisici e infrastruttura – Principali attività | | |
| Servizi *Security* DC – fisici | Vigilanza e sicurezza fisica | Predisposizione degli (eventuali) ulteriori servizi di vigilanza e sicurezza fisica dei DC necessari al PSN. |
| Servizi *Security* DC – infrastruttura | SOC | Predisposizione del SOC (*Security Operation Center*) tramite il quale saranno resi disponibili i servizi di gestione operativa della sicurezza previsti dal Bando di Gara e dall'Offerta. |
| | NOC | Predisposizione di un *Network Operation Center* tramite il quale saranno resi disponibili i servizi di gestione operativa della rete previsti dal Bando di Gara e dall'Offerta. |
| | *Code auditing* | Conduzione dei *test* e delle verifiche necessari alla verifica del codice al fine di prevenire eventuali vulnerabilità (ove possibile, ad es. tecnologie *Open Source*). |
| Servizi *Security* DC – fisici e infrastruttura | Altre attività | Altre attività in ambito *Security* in ottemperanza a quanto previsto dalla Documentazione di Gara e dalle migliorie dell'Offerta. |
| Servizi *Cloud* / CSP – Principali attività | | |
| Servizi *Cloud* / CSP | *Design* e progettazione di dettaglio | Disegno e progettazione di dettaglio dei servizi del PSN.<br>Qualora il servizio preveda il coinvolgimento degli *hyperscaler*, la progettazione sarà effettuata assieme ai loro *team* tecnici in ottica di *co-design*.<br>La progettazione, per ottimizzare le tempistiche di messa a disposizione dei servizi, sarà suddivisa secondo le tipologie di servizio, ovvero *Private Cloud, Secure Public Cloud, Hybrid Cloud on PSN Site, Public Cloud* PSN *Managed*. |
| | Approvvigionamento apparati e predisposizione apparati | Approvvigionamento dei *server* (e loro elementi ancillari) che saranno utilizzati per l'erogazione dei servizi. Predisposizione dei *server* (e loro elementi ancillari). |

| Stream | Attività | Descrizione |
|---|---|---|
| | Allestimento delle piattaforme | Allestimento e configurazione. degli ambienti e delle piattaforme secondo le differenti tipologie di servizio, per garantire una rapida disponibilità dei servizi di infrastruttura. |
| | CSP *Cloud foundation* | Include tutte le attività necessarie alla corretta attivazione ed integrazione dei servizi offerti dai *Cloud Provider* all'interno del PSN. Ad esempio: configurazione ambienti, integrazione rete e sicurezza, attivazione risorse, attivazione *billing*. |
| | Installazione e *Sw integration* | *Deploy* dei *software* ed integrazione degli ambienti necessari per l'erogazione del servizio. |
| | *Test* e collaudo di servizio | Attività di *test* sui servizi per verificarne la correttezza ed operatività. |
| | Risk analysis e VAPT | Analisi dei rischi di sicurezza ed attività di *Vulnerability Assessment* e *Penetration Testing* sui servizi per verificarne la sicurezza. |
| | Test *security* sul dato | Attività di *testing* di sicurezza sui dati. Saranno previsti *test case* diversi a seconda della classificazione dei dati (strategici, critici, ordinari), in modo da verificare la piena corrispondenza con gli obiettivi di sicurezza del PSN. |
| *Onboarding* PA – Principali attività | | |
| *Onboarding* PA | Comunicazione iniziativa PSN | Attività di comunicazione dei servizi resi disponibili dalla NewCo alle PA utenti al fine di massimizzare il numero di PA utenti. |
| | *Tutoring* e formazione verso le PA | Attività legate al *tutoring* ed alla formazione all'uso dei servizi resi disponibili dalla NewCo per le PA utenti. |
| *Onboarding* PA | *Assessment* infrastrutture e servizi | Analisi delle infrastrutture e dei servizi in uso presso le PA utenti per il corretto dimensionamento degli *asset* necessari per l'erogazione dei servizi sulla piattaforma della NewCo. |
| | *Assessment* e classificazione dati (strategici, critici, ordinari) | Analisi delle strutture dati in uso presso le PA utenti per il corretto dimensionamento degli *asset* necessari per l'erogazione dei servizi sulla piattaforma della NewCo. |

| Stream | Attività | Descrizione |
|---|---|---|
| | Sottoscrizione ed adesione | Contrattualizzazione dell'adesione ai servizi offerti dalla NewCo per le PA utenti. |
| | Scelta servizi PSN | Selezione, da parte delle PA utenti, dei servizi del PSN da attivare. |
| *Onboarding* PA | Attività post-Disponibilità dell'Infrastruttura | Attività previste a valle della disponibilità dell'Infrastruttura:<br>• Migrazioni: esecuzione delle migrazioni dei *server* delle PA utenti;<br>• Attivazione dei servizi delle PA utenti;<br>• Controllo, supporto e monitoraggio dello stato di erogazione dei servizi delle PA utenti;<br>• Dismissioni. |

## 1.11 ID CRITERIO:11 – TABELLARE - POSSESSO, IN CAPO AL CONCORRENTE SINGOLO O ASSOCIATO, DELLA CERTIFICAZIONE DI RESPONSABILITÀ SOCIALE ED ETICA SA 8000 O EQUIVALENTE

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|
| 11 | Tabellare | Pari opportunità | Premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31.12.2021 | Possesso, in capo al concorrente singolo o associato, della certificazione idi responsabilità sociale ed etica SA 8000 o equivalente | 2 punti se in possesso della certificazione | **2** |

Miglioramento dell'offerta mediante la disponibilità della certificazione di responsabilità sociale ed etica

| Punteggio indirizzato dall'Offerente = 2 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base:<br><br>certificazione idi responsabilità sociale ed etica SA 8000 o equivalente non strettamente richiesta | Offerente:<br><br>il costituendo RTI dispone della certificazione di responsabilità sociale ed etica SA 8000 |

Con riferimento al criterio n. 11, si dichiara che Fastweb S.p.A., mandataria del RTI, è in possesso della certificazione del sistema di gestione SA 8000, rilasciata da Bureau Veritas Certification, in data 31.12.2021 e valida sino al 30.12.2024. Fastweb S.p.A. si impegna, sin da ora, a compiere ogni attività al fine di garantire la validità della suddetta certificazione per tutta la durata della concessione.
Si allega copia conforme all'originale:

- Relazione tecnica - Allegato 11.1 - Certificato_SA8000.pdf

### 1.12 ID CRITERIO:12 – TABELLARE - IMPIEGO O ASSUNZIONE DI PERSONE CON DISABILITÀ IN QUOTA ECCEDENTE L'OBBLIGO MINIMO DI LEGGE, NELL'ORGANICO DELLA SOCIETÀ DI PROGETTO (NEWCO)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|
| 12 | Tabellare | Pari opportunità | Premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31.12.2021 | Impiego o assunzione di persone con disabilità in quota eccedente l'obbligo minimo di legge, nell'organico della società di progetto (NewCo) | 0,25 punti per ogni unità eccedente l'obbligo minimo di legge fino ad un massimo di 3 punti | **3** |

Con riferimento al criterio n. 12, l'Offerente si impegna affinché l'impiego o assunzione di persone con disabilità, nell'organico della NewCo, sia superiore all'obbligo minimo di legge per una quota eccedente pari a **n. 12 persone.**

Premialità per le pari opportunità di genere e generazionali – persone con disabilità

| Punteggio indirizzato dall'Offerente = 3 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: minimo di legge | **Offerente: 12 persone** con disabilità in quota eccedente il minimo di legge |

### 1.13 ID CRITERIO:13 – TABELLARE - COMPONENTE LAVORO FEMMINILE SUPERIORE AL 10% DELL'ORGANICO DELLA SOCIETÀ DI PROGETTO (NEWCO)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 13 | Tabellare | Pari opportunità | Premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31.12.2021 | Componente lavoro femminile superiore al 10% dell'organico della società di progetto (NewCo) | >10% | 1 punto | 3 |
| | | | | | >20% | 2 punti | |
| | | | | | >30% | 3 punti | |

Con riferimento al criterio n. 13, l'Offerente si impegna affinché la Componente di lavoro femminile **sia superiore al 30%** dell'organico della NewCo.

Premialità per le pari opportunità di genere e generazionali – lavoro femminile

| Punteggio indirizzato dall'Offerente = 3 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: <10% | Offerente: >30% |

## 1.14 ID CRITERIO:14 – TABELLARE - COMPONENTE LAVORO GIOVANILE (ETÀ INFERIORE A 36 ANNI) SUPERIORE AL 5% DELL'ORGANICO DELLA SOCIETÀ DI PROGETTO (NEWCO)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO PARZIALE | | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|---|---|
| 14 | Tabellare | Pari opportunità | Premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31.12.2021 | Componente lavoro giovanile (età inferiore a 36 anni) superiore al 5% dell'organico della società di progetto (NewCo) | >5% | 1 punto | 3 |
| | | | | | >10% | 2 punti | |
| | | | | | >20% | 3 punti | |

Con riferimento al criterio 14, l'Offerente si impegna affinché la Componente di lavoro giovanile (età inferiore a 36 anni) **sia superiore al 20%** dell'organico della NewCo.

Premialità per le pari opportunità di genere e generazionali – lavoro giovanile

| Punteggio indirizzato dall'Offerente = 3 punti | |
|---|---|
| Documentazione di gara | Miglioramento proposto dall'Offerente |
| Valore Base: <5% | Offerente: >20% |

### 1.15 ID CRITERIO:15 – VALUTATIVO - EFFICACIA DELLE MODALITÀ DI VERIFICA PROPOSTE DAL CONCESSIONARIO, MESSE A DISPOSIZIONE DEL CONCEDENTE, PER IL RISPETTO DELLE SEGUENTI NORME E STANDARD EUROPEI IN MATERIA AMBIENTALE (*DO NO SIGNIFICANT HARM*):

- ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD (2020) 55 final);
- Indipendenza energetica e fonti rinnovabili;
- Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE);
- Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva;
- Le procedure di approvvigionamento includeranno la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali;
- Al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della direttiva 2012/19/UE.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 15 | Valutazione | Ambientale | Modalità di verifica del rispetto delle norme ambientali | Efficacia delle modalità di verifica proposte dal Concessionario, messe a disposizione del Concedente, per il rispetto delle seguenti norme e standard europei in materia ambientale (*Do no significant harm*):<br>- ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD(2020) 55 *final*);<br>- Indipendenza energetica e fonti rinnovabili;<br>- Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE);<br>- Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva;<br>- Le procedure di approvvigionamento includeranno la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali;<br>- Al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della direttiva 2012/19/UE. | **3** |

### 1.15.1 Introduzione

La progettazione e la successiva realizzazione del PSN avverrà nell'alveo delle strategie già messe in atto dalle aziende costituenti il RTI in ambito di tutela ambientale. Particolare attenzione sarà rivolta alla implementazione di processi coerenti con le norme e gli *standard* europei di riferimento ed alle modalità di verifica messe a disposizione del Concedente.

### 1.15.2 La strategia ambientale dell'Offerente

#### *1.15.2.1 La Climate Strategy di Fastweb*

La lotta contro i cambiamenti climatici (obiettivo 13) è uno dei 17 obiettivi per lo sviluppo sostenibile (SDGs – *Sustainable Development Goals*) definiti nel 2015 dalle Nazioni Unite con orizzonte 2030, per garantire un futuro sostenibile al nostro Pianeta.

Grazie al suo impegno costante su queste tematiche, descritto meglio in seguito, Fastweb ha conseguito la Certificazione ISO 14064.

Fastweb è, infatti, da anni impegnata su questo fronte, avendo introdotto numerose iniziative per ridurre la propria *Carbon Footprint* e, quindi, il proprio impatto sui cambiamenti climatici.
Sin dal 2014, Fastweb monitora la propria *Carbon Footprint*, seguendo i principali *standard* internazionali in materia.

A partire dal 2015, Fastweb ha convertito l'intero acquisto di energia elettrica, passando, da fonti tradizionali, al 100% di acquisto di energia prodotta da fonti rinnovabili: tale impegno è stato rinnovato fino ad oggi, consentendo all'azienda di evitare di emettere in atmosfera oltre 60.000 ton $CO_2$ ogni anno. Di seguito, sono riportati i Certificati di annullamento relativi all'anno 2020 di tre operatori energetici.



*Figura 22: Certificati di annullamento Fastweb Garanzie d'origine (2020)*

A partire dal 2018, Fastweb ha avviato, inoltre, il calcolo degli ***Enabling Effects*** (*Scope* 4), che rappresentano le emissioni evitate dai clienti grazie all'utilizzo dei servizi erogati: tale analisi permette di quantificare le emissioni evitate sulla base di un modello che considera i servizi di videoconferenza, di *housing* e di *hosting*, di lavoro da remoto e i servizi che consentono ai clienti di evitare la stampa di documenti e di fruire di servizi *online*. Nel 2019, il calcolo degli *Enabling Effects*, effettuato a livello *Corporate*, è stato declinato per singolo servizio, al fine di dare ai clienti un'indicazione puntuale della quantità di emissioni climalteranti evitate grazie all'utilizzo dei servizi Fastweb. A questo scopo è stato sviluppato un modello di calcolo delle emissioni evitate medie per ogni unità di servizio/prodotto commercializzato, le cui assunzioni di base e metodologiche sono state approvate da un *panel* di esperti di Legambiente, che ha ritenuto il documento scientificamente valido e trasparente in coerenza con gli scopi prefissati.
I prodotti e i servizi Fastweb che consentono ai clienti di evitare l'emissione di $CO_2$ sono oggi identificati da una "*Label* di Sostenibilità", sviluppata insieme a Legambiente.

FASTWEB Per la sostenibilità | APPROVATO DA LEGAMBIENTE

### 1.15.2.2 *La Climate Strategy di Aruba*

Aruba da anni porta avanti un piano che ha consentito di essere un'azienda a basso impatto ambientale grazie all'utilizzo di energia proveniente da fonti rinnovabili: dagli investimenti in centrali idroelettriche e impianti fotovoltaici di proprietà, alla progettazione e costruzione di DC con il minimo impatto sull'ambiente.

CLIMATE NEUTRAL DATA CENTER




*Figura 23: Certificato di garanzia rilasciato da Duferco Energia ad Aruba S.p.A.*

Aruba S.p.A. e Duferco Energia S.p.A. hanno sviluppato una *partnership* con la finalità di ricercare soluzioni di risparmio energetico sfruttando tutte le possibilità di ottimizzazione dei consumi. Duferco Energia certifica, attraverso le Garanzie di Origine (GO), che tutta l'energia fornita, viene esclusivamente prodotta da Fonti Rinnovabili.

Aruba ha acquistato centrali Idroelettriche in Italia per poter produrre energia rinnovabile. Questo importante contributo di produzione da fonti rinnovabili ha consentito di portare al minimo l'impatto ambientale della rete di DC:

- Produzione annuale media 35 GWh;
- Potenza complessiva installata 8554 KW.

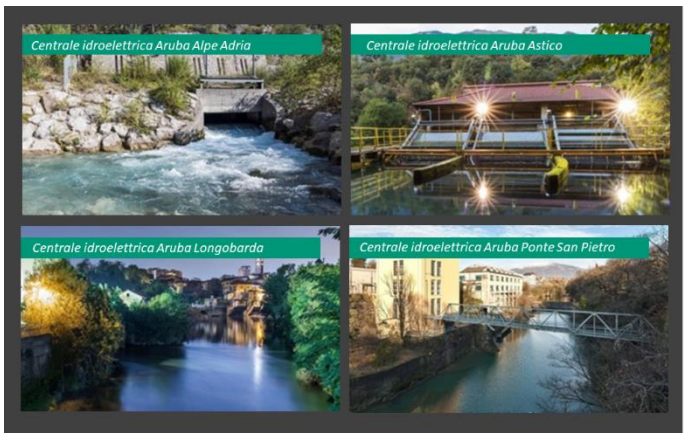



*Figura 24: Centrali idroelettriche acquistate da Aruba in Italia*

## *EMPOWERING* FOTOVOLTAICO

I DC Aruba acquisiscono l'energia pulita del sole, grazie a pannelli fotovoltaici installati su tutta la superficie utile e meglio esposta alla luce dei nostri edifici, segnatamente:

- 10.258 mq pannelli installati in copertura;
- potenza complessiva 2310 KW.



*Figura 25: Pannelli fotovoltaici installati sui DC*

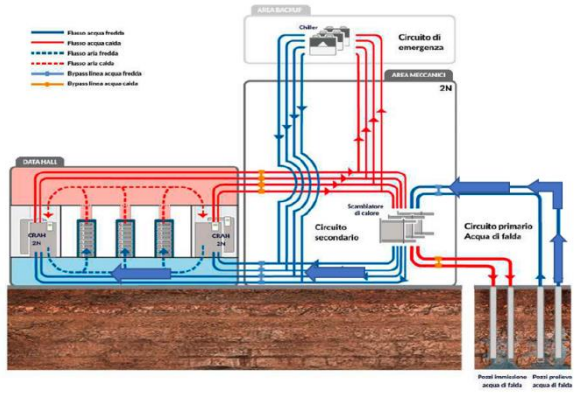



*Figura 26: Impianto geotermico per i sistemi di raffreddamento degli apparati*

### IMPIANTO GEOTERMICO

Le risorse geotermiche del sottosuolo consentono di ottenere un livello di efficienza avanzata per i sistemi di raffreddamento degli apparati. L'acqua di falda viene prelevata da due pozzi distinti e reimmessa nel sottosuolo dopo lo scambio termico.

### DYNAMIC FREE COOLING

Con le basse temperature, il *Dynamic Free Cooling* permette di risparmiare energia utilizzando l'aria esterna, opportunamente filtrata, per raffreddare la sala *server*. L'aria calda viene espulsa dall'edificio da grandi ventilatori, serrande elettriche chiudono ed aprono all'occorrenza le aperture.

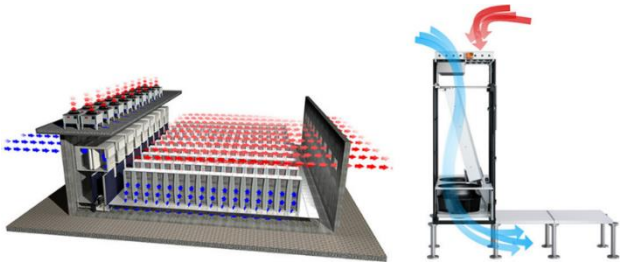


*Figura 27: Funzionamento del Dynamic Free Cooling*

## 1.15.3 Modalità di verifica proposte per il rispetto delle norme e standard europei relativamente al principio del "*Do Not Significant Harm*" (DNSH)

Relativamente al principio del "*Do Not Significant Harm*" (DNSH), l'Offerente si impegna al rispetto dei requisiti previsti in relazione a *standard* e normative del settore attraverso l'adempimento delle richieste specifiche, unitamente alla valutazione e monitoraggio del raggiungimento degli obiettivi prefissati.

In particolare, l'Offerente si impegna - e farà sì che la Newco provveda - a mettere a disposizione del Concedente tutta la documentazione a supporto delle modalità di verifica attuate o pianificate, unitamente alla dimostrazione della loro efficacia. Per consentire una efficace modalità di consultazione della documentazione attestante il rispetto dei requisiti, l'Offerente intende mettere a disposizione del Concedente un portale che consenta di visualizzare e monitorare lo stato di avanzamento, gli aggiornamenti e i *report* periodici, in ogni momento. L'obiettivo che ci si pone è quello di avere sempre a disposizione una *repository* aggiornata all'interno della quale sia il Concessionario che il Concedente possano scambiarsi tutte le informazioni e documentazione a supporto delle specifiche esigenze di verifica (ad esempio, politica energetica, procedure di rendicontazione delle emissioni, progettazione DC, specifiche tecniche, progettazione, schede tecniche materiali/tecnologie utilizzate, certificazioni di prodotto rilasciate dai fornitori, ecc.). All'interno del portale, sarà strutturata una sezione dedicata al rispetto del principio del DNSH, specifica per ogni *standard* e normativa di settore citata nel prosieguo del presente paragrafo. Nella specifica sezione, sarà possibile aggiungere ed aggiornare le *check list* di verifica e controllo per ciascun settore di intervento, che

riassumono i principali elementi di verifica richiesti nella corrispondente scheda tecnica di riferimento, in modo tale da fornire tutte le informazioni operative e normative che identificano i requisiti tassonomici, ossia i vincoli DNSH, e nelle quali sono riportati i riferimenti normativi, i vincoli ed elementi di verifica.

All'interno del portale sarà, quindi, possibile consultare, per ogni ambito di intervento, la seguente documentazione minima, atta a verificare il rispetto del principio DNSH:

- Autocertificazioni mediante compilazione di *check list* di controllo, laddove specificatamente richieste come modalità di verifica del principio DNSH;
- Documentazione a supporto dell'implementazione delle *Best Practice* di settore;
- Certificazioni conseguite per il rispetto degli *standard* (ad es. UNI EN ISO 14001, UNI EN ISO 14064, UNI CEI EN ISO 50001, etc.);
- Documentazione a supporto e *report* sugli esiti delle attività di verifica effettuate (es. audit interni/esterni);
- Documentazione a supporto e specifiche tecniche relative ai sistemi di monitoraggio adottati;
- Documentazione relativa a specifici ambiti di valutazione/intervento, laddove richiesti (es. sostanze pericolose);
- Documentazione di dettaglio richiesta da specifici *standard* (ad es. analisi dei rischi per ISO/IEC TS 22237);
- Documentazione a dimostrazione dell'utilizzo di apparecchiature con marcatura CE (in conformità alla Direttiva 2009/125/CE);
- Documentazione a dimostrazione della corretta gestione dei materiali a fine vita (RAEE) in conformità alle prescrizioni della DIRETTIVA 2012/19/UE (e relativa attuazione tramite il D. Lgs. 49/2014);
- Pianificazione delle verifiche periodiche (es. *audit* interni/esterni) previste per il mantenimento e rinnovo delle certificazioni conseguite;
- Pianificazione delle attività previste per il raggiungimento degli obiettivi definiti per il rispetto dei requisiti e il miglioramento delle *performance* in merito alle tematiche analizzate durante le verifiche periodiche;
- *Report* periodico indicante le azioni intraprese, gli obiettivi raggiunti e i benefici ottenuti (rappresentati, ad esempio, dalla percentuale di riduzione/compensazione delle emissioni in riferimento alla UNI EN ISO 14064, etc..) relativamente alle attività pianificate;
- Certificazioni di fornitura in Garanzia di Origine, unitamente a documentazione tecnica disponibile in merito a produzione ed auto-consumo di energia proveniente da fonti rinnovabili.

Inoltre, per fornire un maggior dettaglio degli obiettivi raggiunti dal Concessionario, all'interno del portale si metterà a disposizione la sezione degli *Environmental Target Plan*, nella quale verranno esposti i *target* che il Concessionario ha intenzione di raggiungere per l'anno n, e, all'anno n+1, si pubblicherà la percentuale di raggiungimento di tali *target* e verranno esposti i nuovi obiettivi.

Ad ulteriore comprova dell'impegno dell'Offerente, verranno pubblicate tutte le azioni di compensazione delle emissioni, introdotte per il *Net Zero* del servizio erogato al Concedente ed alle Amministrazioni utenti ed il relativo bilancio delle emissioni prodotte/compensate/ridotte relativamente al servizio stesso.

Nei seguenti paragrafi, si evidenziano, per ogni ambito di intervento, le specifiche modalità di verifica prescritte dalle schede tecniche e relative *check list*, così come definite dalla "*Guida operativa per il rispetto del principio di non arrecare danno significativo all'ambiente*". Inoltre, si fornisce un dettaglio delle azioni che l'Offerente si impegna a intraprendere in merito al rispetto delle singole norme/*standard*.

### 1.15.4 ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD (2020) 55 final)

#### *1.15.4.1 Modalità di Verifica dello Standard UNI EN ISO 14001*

Lo *standard* UNI EN ISO 14001 definisce i requisiti di un Sistema di Gestione Ambientale implementabile all'interno dell'organizzazione e prevede la relativa certificazione a seguito di verifica da parte di un ente terzo accreditato. Lo *standard* prevede monitoraggio, misura, analisi e valutazione della prestazione ambientale da parte dell'organizzazione.

Relativamente alla **modalità di verifica** dei requisiti, l'organizzazione è tenuta alla conduzione, ad intervalli pianificati, di *audit* interni allo scopo di fornire informazioni utili all'accertamento di conformità del proprio Sistema di Gestione Ambientale, unitamente all'efficacia delle azioni di attuazione e mantenimento dello stesso.
La frequenza delle valutazioni può variare in base a condizioni esterne ed interne dovute, principalmente, a modifiche delle condizioni operative, degli obblighi di conformità e delle prestazioni riportate nelle precedenti verifiche.
L'Offerente, pertanto, metterà a disposizione del Concedente un *report* relativo alla NewCo, con le principali evidenze emerse dagli *audit* interni e dal processo di riesame, oltre a dettagliarne gli obiettivi raggiunti ed a comunicare il rinnovo della certificazione tramite opportuna certificazione.

In relazione al principio del *Do Not Significant Harm* **(DNSH)**, relativamente al rispetto delle prescrizioni della ISO 14001, vengono, di seguito, riportate le principali evidenze:

- la ***scheda tecnica n.3 "Acquisto,* Leasing *e Noleggio di* computer *ed apparecchiature elettriche ed elettroniche"*** (la "Scheda 3") **richiede la certificazione UNI EN ISO 14001** nella fase di verifica *ex-ante* per il rispetto del vincolo n.4 del DNSH "*Economia circolare*" e, in particolare, viene richiesta la rispondenza della qualità di processo di ricondizionamento/rifabbricazione in conformità con lo *Standard* ISO 14001;
- all'interno delle ***schede tecniche n.6 "Servizi informatici di hosting e cloud"*** (la "Scheda 6") ***e n.8 "Data Center"*** (la "Scheda 8") viene richiesto, nella fase di verifica *ex-ante*, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatico*", lo svolgimento di studi di fattibilità per l'implementazione e il rispetto di tutte le "*pratiche attese*" incluse nella versione più recente del codice di condotta europeo sull'efficienza energetica dei centri dati (il "**Codice di condotta DC**"). A tal riguardo, le *general policies* sul "*Data Centre Utilisation, Management and Planning*" del JRC *Technical Report* "2021 ***Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency" in merito all'environmental management per il Data Center, richiamano lo standard ISO 14001*** come riferimento per le metodologie e *guidelines* internazionali da seguire per la pianificazione delle pratiche di *environmental management* sui *Data Center*.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH, la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di verifica e controllo** della Scheda 3, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura: Certificazione della qualità del processo di ricondizionamento/rifabbricazione in conformità con lo *standard* ISO 14001.
Inoltre, Il rispetto dei vincoli DNSH relativamente alle schede tecniche n.3 "*Acquisto,* Leasing *e Noleggio di computer ed apparecchiature elettriche ed elettroniche*" e n.8 "*Data center*", sarà verificato attraverso l'ottenimento e corretta archiviazione di tutta la documentazione richiesta dalla specificità della misura: studi di fattibilità per l'implementazione e il rispetto di tutte le

"*pratiche attese*", incluse nella versione più recente del Codice di condotta DC, in rispondenza delle linee guida europee e metodologie *standard* internazionali in ambito di *environmental management*.

#### 1.15.4.1.1 Il Sistema di Gestione Ambientale certificato UNI EN ISO 14001– Stato attuale ed azioni future

Le aziende del costituendo RTI posseggono la certificazione UNI EN ISO 14001:

- la certificazione ISO 14001 di Fastweb è stata rilasciata per la prima volta in data 28/12/2007, con ultimo *audit* di sorveglianza annuale completato in data 27/07/2021.
- la certificazione ISO 14001 di Aruba è stata rilasciata per la prima volta a settembre 2017, con ultimo *audit* di sorveglianza a ottobre 2021.

### *1.15.4.2 Modalità di verifica dello standard UNI EN ISO 14064*

Lo *standard* UNI EN ISO 14064 relativo alle emissioni di gas ad effetto serra rappresenta una norma volontaria e prevede la relativa certificazione a seguito di verifica da parte di un ente terzo accreditato.
Relativamente alla **modalità di verifica** dei requisiti presentati, l'Offerente, potendo decidere volontariamente di effettuare la verifica delle informazioni sulle emissioni di gas a effetto serra in forma imparziale e obiettiva, in coerenza con i principi descritti nella parte UNI EN ISO 14064, metterà a disposizione del Concedente un *report* in cui saranno quantificate periodicamente le emissioni in tonnellate di $CO_2$eq prodotte ed evitate dalla Newco (in termini di riduzione e compensazione).

In relazione al principio del **DNSH**, relativamente al rispetto delle prescrizioni della UNI EN ISO 14064, vengono di seguito riportate le principali evidenze:

- nella scheda tecnica n.15 "*Produzione e stoccaggio di idrogeno in aree industriali dismesse*" (la "**Scheda 15**") e scheda tecnica n.16 "*Produzione e stoccaggio di Idrogeno nei settori* Hard to Abate" (la "**Scheda 16**") viene richiesto, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatici*", che vengano rispettati i principi e le indicazioni presenti nella UNI EN ISO 14064 per la valutazione e rendicontazione della riduzione delle emissioni di gas serra, che dovrà essere calcolata come previsto dal Regolamento (UE) 2018/842 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo alle riduzioni annuali vincolanti delle emissioni di gas serra a carico degli Stati membri nel periodo 2021-2030, facente riferimento alla Direttiva 2003/87/CE del Parlamento Europeo, o, in alternativa, mediante la norma UNI EN ISO 14067 (*carbon footprint*) o UNI EN ISO 14064 (*quantification and reporting of* GHG).

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH**, la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di Controllo delle Schede 15 e 16, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura: misurazione della riduzione di gas a effetto serra mediante l'utilizzo della norma UNI EN ISO 14064.

#### 1.15.4.2.1 La certificazione UNI EN ISO 14064 – Stato attuale ed azioni future

Fastweb è già in possesso della certificazione EN ISO 14064, mentre Aruba ha avviato il processo di certificazione con l'obiettivo di conseguirla entro Q2 2022.

#### *1.15.4.3 Modalità di verifica dello standard UNI CEI EN ISO 50001*

Lo *standard* UNI CEI EN ISO 50001 definisce i requisiti per l'implementazione e il miglioramento di un Sistema di Gestione dell'Energia ("SGE") consentendo alle organizzazioni di perseguire il miglioramento continuo delle prestazioni energetiche con approccio sistematico nel rispetto degli adempimenti legali.

Relativamente alla **modalità di verifica** dei requisiti presentati, l'Offerente è tenuto ad effettuare un *audit* preliminare esterno al fine di determinare la conformità dell'organizzazione rispetto ai requisiti dello *standard*. Tale fase si conclude con eventuali osservazioni per il raggiungimento della conformità.
La certificazione UNI EN ISO 50001 viene rilasciata a seguito di esito positivo di *audit* di certificazione eseguito da organismo accreditato relativo alla verifica della conformità del sistema di gestione rispetto ai requisiti previsti dallo standard. L'Offerente metterà a disposizione del Concedente tale certificazione relativa ai DC utilizzati dalla NewCo. Inoltre, a seguito del conseguimento della certificazione, l'organizzazione è tenuta ad effettuare *audit* di sorveglianza annuale per il monitoraggio del mantenimento del sistema di gestione e la valutazione dei miglioramenti ottenuti, atti a determinare il raggiungimento degli obiettivi in termini di *energy management*, per cui la NewCo metterà a disposizione del Concedente un *report* con gli obiettivi annuali raggiunti in termini di miglioramento delle prestazioni. Al termine del periodo di validità della certificazione, pari a tre anni, l'organizzazione è tenuta ad effettuare un *audit* di rinnovo al fine di confermare il certificato per un ulteriore triennio.

In relazione al principio del DNSH, relativamente al rispetto delle prescrizioni della UNI EN ISO 50001, vengono di seguito riportate le principali evidenze:

- All'interno della **Scheda 6 e della Scheda 8** viene richiesto nella fase di verifica *ex ante*, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatico*", lo svolgimento di studi di fattibilità per l'implementazione e il rispetto di tutte le "*pratiche attese*" incluse nella versione più recente del Codice di condotta DC. A tal riguardo, le ***general policies* sul "*Data Centre Utilisation, Management and Planning*" del JRC Technical Report "2021 *Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency*", richiamano lo *standard* ISO 50001 come riferimento** per le metodologie e *guidelines* internazionali da seguire per la pianificazione delle pratiche di *energy management* sui DC.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH, la NewCo metterà a disposizione del Concedente un'autocertificazione realizzata mediante la compilazione della *Checklist* di verifica e controllo** delle Schede 6 e 8, unitamente all'ottenimento e corretta archiviazione di tutta la documentazione richiesta dalla specificità della misura: studi di fattibilità per l'implementazione e il rispetto di tutte le "*pratiche attese*" incluse nella versione più recente del Codice di condotta DC, in rispondenza delle linee guida europee e metodologie *standard* internazionali in ambito di *energy management* (di cui, un esempio è rappresentato dallo standard ISO 50001).

##### 1.15.4.3.1 Il Sistema di Gestione dell'Energia certificato UNI CEI EN ISO 50001 – Stato attuale ed azioni future

I *Data Center* DC1 e DC2 sono certificati ISO 50001 alla data, mentre per DC3 e DC4 la certificazione è prevista entro 18 mesi.

#### 1.15.4.4 SWD (2020): Criteri dell'UE in materia di appalti pubblici verdi per i centri dati, le sale server e i servizi cloud

I criteri dell'UE in materia di appalti pubblici verdi (*Green Public Procurement*, GPP) hanno lo scopo di agevolare l'acquisto di beni, servizi e lavori a ridotto impatto ambientale da parte delle autorità pubbliche. Il Documento di lavoro dei servizi della Commissione recante "*Criteri dell'UE in materia di appalti pubblici verdi per i centri dati, le sale server e i servizi cloud*" - SWD (2020) 55 *Final* (i "**Criteri SWD 55**") elenca i criteri GPP dell'UE per i centri dati, le sale *server* e i servizi *cloud*. Vengono, di seguito, riportate le principali evidenze in termini di verifica delle prescrizioni:

**Utilizzo dei *server***

La NewCo deve possedere competenze ed esperienza pertinenti in relazione all'ottimizzazione dell'utilizzo dei *server*. Ciò deve comprendere servizi di virtualizzazione dei *server*, strumenti e *software* di gestione dell'utilizzo e il consolidamento delle risorse informatiche nei DC.

**Controllo delle sostanze pericolose - sostanze soggette a restrizioni in *server*, apparecchiature di archiviazione dati e di rete**

La NewCo, anche tramite l'Offerente, deve dimostrare che sono effettuati controlli sulle sostanze soggette a restrizioni lungo la catena di approvvigionamento per i prodotti da fornire.

**Gestione del fine vita per *server*, apparecchiature di archiviazione dati e di rete**

La NewCo si deve dotare di un servizio per:

- il riutilizzo o il riciclaggio dell'intero prodotto;
- il trattamento selettivo dei componenti conformemente all'allegato VII della Direttiva RAEE per le apparecchiature che hanno raggiunto il termine della propria vita utile;
- il riciclaggio dei componenti al fine di recuperare materie prime essenziali.

**Monitoraggio ambientale**

L'Offerente deve mettere a disposizione della NewCo, tutto il necessario al fine di dimostrare che la struttura possegga servizi ed infrastrutture per il controllo ambientale in linea con i requisiti e le raccomandazioni della norma EN 50600-2-3.

**Migliori prassi per il sistema di raffreddamento – DC esistenti adibiti a servizi di coubicazione o di *hosting***

L'Offerente deve mettere a disposizione della NewCo, tutto il necessario al fine di dimostrare che il DC integri le migliori prassi "previste" in merito a:

- gestione e progettazione del flusso di aria;
- impianto di raffreddamento;
- condizionatori d'aria/unità per il trattamento dell'aria nelle sale *computer*.

**Fattore di energia rinnovabile (*Renewable Energy Factor*, REF)**

Il fattore di energia rinnovabile del DC deve essere uguale a 1 (100 % rinnovabile).

In relazione al principio del DNSH, relativamente al rispetto delle prescrizioni dei Criteri SWD 55, vengono, di seguito, riportate le principali evidenze:

- nella guida operativa per il rispetto del principio del DNSH, all'interno della Scheda 6 e della Scheda 8, vengono indicati i Criteri SWD 55 come normativa di riferimento per la definizione dei criteri per garantire il rispetto del DNSH.
  Inoltre, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatico*", in un primo momento, è richiesto, il rispetto dei seguenti criteri di esecuzione del contratto, definiti dai Criteri SWD 55:
  - monitoraggio dell'utilizzo delle attrezzature informatiche;

- comunicazione della destinazione finale di *server*, apparecchiature di archiviazione dati e di rete;
- dimostrazione dell'efficienza dell'uso dell'energia (PUE) al momento della consegna;
- implementazione progressiva della certificazione per l'efficienza energetica, *Energystar* o equivalente, per tutte le nuove apparecchiature IT.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH, la NewCo metterà a disposizione del Concedente un'autocertificazione realizzata mediante la compilazione della *Checklist* di verifica e controllo** delle Schede 6 e 8, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura: fornire la prova dell'attuazione dei criteri di esecuzione del contratto così come definiti dai Criteri SWD 55.

#### *1.15.4.5 Modalità di verifica degli standard EN 50600 e ISO/IEC TS 22237 per i Data Center*

Gli *standard* EN 50600 ed ISO/IEC TS 22237 rappresentano i primi *standard* che utilizzano un approccio omnicomprensivo ed esaustivo in termini di specifiche per la costruzione e l'esercizio di DC.
La conformità con lo *standard* EN 56000 o ISO 22237 richiede:

- analisi dei rischi;
- definizione della classe di disponibilità in base alle risultanze dell'analisi dei rischi;
- definizione del livello di sicurezza in base alle risultanze dell'analisi dei rischi;
- definizione del livello di efficienza energetica.

##### 1.15.4.5.1 Codice di Condotta DC

La EN50600 ha integrato il Codice di Condotta DC sviluppato dalla Comunità Europea. L'obiettivo è quello di informare e stimolare gli operatori e i proprietari di DC a ridurre il consumo di energia in modo efficace dal punto di vista dei costi senza ostacolare la funzione *mission critical* dei DC stessi.
Il Codice di condotta DC mira a raggiungere questo obiettivo migliorando la comprensione della domanda di energia all'interno del DC, aumentando la consapevolezza e raccomandando *best practice* e obiettivi di efficienza energetica.

Relativamente alla **modalità di verifica** dei requisiti presentati, si evidenziano i seguenti aspetti:

- la certificazione secondo EN 50600 è volontaria, vale a dire che, attualmente, non esiste un requisito legale o normativo per la certificazione;
- i documenti principali della serie EN 50600 sono stati portati sulla ISO TS 22237 che diventerà, in un prossimo futuro, lo *standard* certificabile;
- quando verrà definito il percorso di accreditamento questo sarà gestito, come per le altre norme ISO/IEC/UNI, dagli enti di accreditamento nazionali riconosciuti.

La EN 50600/ISO 22237 richiede, come primo passo, una analisi dei rischi secondo le linee guida ISO 31010.

In relazione al principio del DNSH, vengono, di seguito, riportate le principali evidenze:

- all'interno delle **Schede 6 e 8**, viene richiesto, nella fase di verifica *ex-ante*, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatico*", che i DC **aderiscano alle pratiche raccomandate contenute nel CEN-CENELEC documento CLC TR50600-99-1 "*Data centre facilities and infrastructures- Part* 99-1 : *Recommended practices for energy management*" o alle "*pratiche attese*" incluse nella versione più recente del Codice

di condotta DC, segnatamente le "*Best Practice Guidelines for the European Code of Conduct for Data Centre Energy Efficiency* » 2021 (JRC)

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH, la NewCo metterà a disposizione del Concedente un'autocertificazione realizzata mediante la compilazione della *Checklist* di verifica e controllo** delle Schede 6 e 8, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura.

#### 1.15.4.5.2 Gli *standard* EN 50600 e ISO/IEC TS 22237 per i *Data Center* – Stato attuale ed azioni future

L'Offerente si impegna all'adesione, da parte della NewCo, al Codice di condotta DC attraverso un percorso di valutazione relativo alle *best practice* implementate nei DC del PSN e la verifica della conformità rispetto alle indicazioni dei principi espressi nelle linee guida, avendo riscontrato, a seguito di analisi di dettaglio, la totale rispondenza ai requisiti per gli elementi di cui presenta disponibilità diretta. Inoltre, in merito alla certificazione ISO/IEC TS 22237, l'Offerente ha avviato un percorso di valutazione relativamente ai requisiti previsti dallo *Standard* e *Gap Analysis* al fine di ottenere la Dichiarazione di Conformità.

### *1.15.4.6 Modalità di verifica per il monitoraggio del PUE*

Il ***Power Usage Effectiveness* (PUE)** è considerato la metrica principale per misurare l'efficienza energetica dell'infrastruttura di un DC. Il PUE è definito come il rapporto tra la totale energia consumata dal sito e l'energia consumata dalle apparecchiature IT.

La *"Green Grid Association"* ha pubblicato una serie di regole e linee guida riguardanti il processo da seguire per la misurazione del PUE.

Il PUE può essere calcolato e monitorato con tre diversi livelli di approccio: L1 *Basic*, L2 *Intermediate*, L3 *Advanced* a seconda del:

- punto di misura dell'IT *Equipment;*
- frequenza di calcolo e monitoraggio come riportato nella tabella seguente (Tabella 7).

*Tabella 7: A comprehensive examination of the metric - White Paper #49, The Green Grid*

| | **Level 1 (L1) Basic** | **Level 2 (L2) Intermediate** | **Level 3 (L3) Advanced** |
|---|---|---|---|
| **IT Equipment Energy** | UPS Outputs | PDU Outputs | IT Equipment Input |
| **Total Facility Energy** | Utility Inputs | Utility Inputs | Utility Inputs |
| **Measurement Interval** | Monthly/Weekly | Daily/Hourly | Continuous (15 minutes or less) |

In relazione alla necessaria **metodologia di verifica** si evidenzia che la *Green Grid Association*, la cui metodologia di misurazione della metrica è internazionalmente riconosciuta, classifica i risultati PUE riportati pubblicamente utilizzando quattro categorie: Non riconosciuto (*Unrecognized*), Segnalato (*Reported*), Registrato (*Registered*) e Certificato (*Certified*). La tabella sotto riportata (Tabella 8) fornisce le descrizioni di queste categorie.

*Tabella 8: Classificazione dei risultati PUE secondo la Green Grid Association*

| CLASSIFICAZIONE | DESCRIZIONE |
|---|---|
| *Unrecognized* | Risultato riportato pubblicamente senza pretese di seguire le linee guida di *The Green Grid*. *The Green Grid* non commenterà risultati non riconosciuti. |
| *Reported* | Risultato riportato pubblicamente da un'organizzazione che dichiara di aver seguito le raccomandazioni di misurazione e le linee guida della nomenclatura di *The Green Grid*. *The Green Grid* non commenterà i risultati riportati. |
| *Registered* | Risultato riportato pubblicamente, con dati contestuali chiave forniti a *The Green Grid* dall'organizzazione che effettua la segnalazione, utilizzando il database delle prestazioni dei DC di *The Green Grid*. |
| *Certified* | Risultato riportato pubblicamente, con dati aggiuntivi chiave richiesti per la convalida di terzi o certificazione dei risultati, fornito a *The Green Grid* da parte dell'organizzazione segnalante. |

In relazione al principio del DNSH, relativamente al monitoraggio del PUE, si evidenzia che sia la Scheda 6, sia la Scheda 8 richiedono, come elemento di verifica *ex-post*, per il rispetto del vincolo n.1 del DNSH "*Mitigazione del cambiamento climatico*", la prova dell'attuazione dei criteri di esecuzione del contratto. La citata esigenza è definita dai Criteri SWD 55. A tal proposito, è richiesta la dimostrazione dell'efficienza dell'uso dell'energia tramite il monitoraggio del PUE al momento della consegna.
Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH**, la NewCo metterà a disposizione del Concedente un'autocertificazione, mediante compilazione della *Checklist* di Controllo delle Schede 6 e 8. Inoltre, sarà prevista la corretta archiviazione e messa a disposizione di tutta la documentazione relativa alla specificità della misura.

#### 1.15.4.6.1 Il monitoraggio del PUE – Stato attuale ed azioni future

La NewCo adotterà per i DC del PSN un approccio misto per la misura del PUE:

- L1 per i punti di misura dell'IT *Equipment*: la misura dell'energia dei *server* avviene a valle degli UPS attraverso il monitoraggio di 20 *power meter* (10 per ramo) che alimentano le rispettive blindosbarre da cui le PDU dei clienti prelevano l'energia;
- L2 o L3 per l'intervallo di misura temporale: il DCIM campiona i dati delle misure con frequenza inferiore al minuto pertanto è possibile calcolare il PUE con l'intervallo temporale desiderato. Solitamente, i dati vengono estratti con campionamento 15 minuti (stesso campionamento utilizzato dai distributori elettrici per la fornitura dei dati in bolletta).

### *1.15.4.7 Modalità di verifica per determinare l'indipendenza energetica e l'utilizzo di fonti rinnovabili*

Il Decreto Legislativo 3 marzo 2011, n.28 e ss.mm.ii. (il "**D.Lgs. 28/11**") in attuazione della direttiva 2009/28/CE sulla promozione dell'uso dell'energia da fonti rinnovabili, recante modifica e successiva abrogazione delle direttive 2001/77/CE e 2003/30/CE, all'articolo 11, istituisce l'obbligo di integrazione delle fonti rinnovabili negli edifici di nuova costruzione e negli edifici esistenti sottoposti a ristrutturazioni rilevanti.
La Guida operativa riguardante il principio del DNSH presenta riferimenti in merito alla promozione della produzione/utilizzo di energia da fonti rinnovabili tramite la normativa di riferimento Direttiva EU 2018/2001 ("**RED II**") sulla promozione dell'uso dell'energia da fonti rinnovabili.

- All'interno della **scheda tecnica n.5 "Interventi edili e cantieristica generica non connessi con la costruzione/rinnovamento di edifici"** (la "**Scheda 5**") viene richiesta, nella fase di verifica *ex ante*, per il rispetto del vincolo n.1 del DNSH *"Mitigazione del cambiamento*

*climatico*", la **dichiarazione del fornitore di energia elettrica relativamente all'impegno di garantire fornitura elettrica prodotta al 100% da fonti rinnovabili.**

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH,** la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di Controllo della Scheda 5, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura: dichiarazione del fornitore di energia elettrica relativamente all'impegno di garantire fornitura elettrica prodotta al 100% da fonti rinnovabili.

#### 1.15.4.7.1 Indipendenza energetica e fonti rinnovabili – Stato attuale ed azioni future

L'Offerente ha già convertito l'intero acquisto di energia elettrica, passando da fonti tradizionali al 100% di acquisto di energia prodotta da fonti rinnovabili (certificata da Garanzia d'Origine dal fornitore) ed è in grado di contribuire parzialmente al proprio fabbisogno energetico attraverso gli impianti di seguito descritti:

- FASTWEB - Impianti fotovoltaici installati in alcuni siti per un totale di 200 kW picco installati. Inoltre, come impegno per il futuro, l'avvio di un piano per la realizzazione di impianti fotovoltaici ("**FV**") che interessano le centrali di telecomunicazione distribuite in tutta Italia con caratteristiche idonee ad ospitare un impianto FV.
- ARUBA - Il 12% del fabbisogno energetico del DC2 viene prodotto tramite:
  - Centrale idroelettrica nel DC di Ponte san Pietro (BG)
  - Impianto FV dedicato.
  - Utilizzo di acqua di falda a temperatura 10-15°C come *cooling system* permettendo una riduzione significativa dell'utilizzo dei *chiller* di impianto.

#### *1.15.4.8 Modalità di verifica relative all'applicazione della direttiva sulla progettazione ecocompatibile (direttiva 2009/125/CE);*

La direttiva europea sulla Progettazione ecocompatibile 2009/125/CE, denominata ***Ecodesign Directive – Energy related product*** **("Direttiva ErP"),** stabilisce un quadro normativo per l'immissione di apparecchiature connesse all'energia sul mercato europeo. Garantisce la possibilità di armonizzare, a livello comunitario, le specifiche per la progettazione ecocompatibile di tutti i prodotti significativi relativi all'energia, riguardando qualsiasi bene che abbia un impatto sul consumo energetico durante l'utilizzo, incluse le parti destinate a essere integrate nei prodotti.

La Direttiva ErP richiede che i produttori di apparecchiature che consumano energia svolgano attività di *ecodesign*, sviluppando prodotti mediante criteri orientati alla riduzione degli impatti ambientali lungo tutte le fasi del ciclo di vita del prodotto, attraverso l'utilizzo della "*Valutazione del Ciclo di Vita*".

Il rispetto del principio del DNSH, per quanto concerne la Direttiva ErP, è garantito se sono assicurate le richieste delle Schede 6 e 8 di seguito descritte:

- La Scheda 6 richiede, per il rispetto del vincolo n. 4 del DNSH "*Economia Circolare*", che i *server* e i DC selezionati per l'erogazione dei servizi siano realizzati secondo i criteri previsti nella Direttiva ErP;
- La Scheda 8 richiede, per il rispetto del vincolo n. 4 del DNSH "*Economia Circolare*", che l'attrezzatura utilizzata rispetti i criteri per la progettazione ecocompatibile di *server* e prodotti di archiviazione dati previsti nel Regolamento (UE) 2019/424 della Commissione del 15 marzo 2019 e modifiche comprese nel Regolamento (UE) 2021/341 della Commissione e nella Direttiva ErP.

In merito alla **metodologia di verifica** della progettazione ecocompatibile**,** la Direttiva ErP, nell'allegato IV, descrive la procedura con la quale il fabbricante o il suo mandatario assicurano

e dichiarano che il prodotto soddisfa le pertinenti prescrizioni della misura di esecuzione applicabile. Le indicazioni pratiche per l'applicazione della Direttiva ErP sono contenute nei Regolamenti sopra citati (Regolamento (UE) 2019/424 della Commissione del 15 marzo 2019 e modifiche comprese nel Regolamento (UE) 2021/341 della Commissione e nella Direttiva ErP). Essi definiscono, infatti, norme specifiche per ogni categoria di prodotto, fissando misure di esecuzione generali e particolari.

Il fabbricante deve compilare un modulo di documentazione tecnica che consenta una valutazione della conformità del prodotto alle prescrizioni della misura di esecuzione applicabile, impegnandosi ad adottare tutte le misure necessarie a garantire che il prodotto sia fabbricato conformemente alle specifiche di progettazione ed alle prescrizioni della misura ad esso applicabile. Tutte le misure adottate dal fabbricante per migliorare le prestazioni ambientali complessive del prodotto ed elaborare il profilo ecologico di un prodotto, se richiesto dalla misura di esecuzione, attraverso la progettazione e la fabbricazione, devono essere documentate in maniera sistematica e ordinata sotto forma di istruzioni e procedure scritte inserite anche nella Dichiarazione CE di conformità.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH**, la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di Controllo delle Schede 6 e 8, unitamente all'ottenimento e corretta archiviazione di tutta la documentazione richiesta.

#### 1.15.4.8.1 Il rispetto della Direttiva ErP da parte del RTI – Stato attuale ed azioni future

Con riferimento alla Direttiva ErP, attuata in Italia dal D. Lgs. n. 15/2011 e ss.mm.ii. (il "**D.Lgs. 15**"), relativa all'istituzione di un quadro per l'elaborazione di specifiche per la progettazione ecocompatibile dei prodotti connessi all'energia, il RTI si impegna a far utilizzare dalla NewCo, nell'ambito del contratto, dispositivi ed apparecchiature conformi ai requisiti definiti sia a livello europeo, che a livello nazionale.
In particolare, tutti gli apparati presenti nei DC saranno dotati di marcatura CE conforme all'Allegato I del D.Lgs. 15 e di dichiarazione CE di conformità, con la quale il fabbricante o il suo mandatario autorizzato o, in assenza di quest'ultimo, l'importatore, garantiscono e dichiarano che il prodotto rispetta tutte le pertinenti disposizioni della misura di esecuzione applicabile, ovvero del provvedimento che dà attuazione alla medesima misura. Tali attestazioni sono relative al rispetto dei criteri di efficienza energetica e di progettazione ecocompatibile definiti dalla Direttiva ErP e dal D.Lgs.15.

### *1.15.4.9 Modalità di verifica per accertare che le apparecchiature elettriche acquistate non contengano sostanze soggette a restrizione elencate nell'allegato II della Direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale Direttiva*

La Direttiva 2011/65/UE (la "**Direttiva RoHS**") limita l'uso di piombo (Pb), mercurio (Hg), cadmio (Cd), cromo esavalente (Cr6+), bifenili polibromurati (PBB) ed eteri di difenil polibrominato (PBDE) nella produzione di alcune delle apparecchiature elettriche ed elettroniche vendute nell'Unione Europea. La Direttiva RoHS impone l'obbligo della marcatura CE e della dichiarazione di conformità UE prima di immettere sul mercato apparecchiature elettriche ed elettroniche ("**AEE**").

Il rispetto del principio del DNSH, per quanto concerne la Direttiva RoHS, è garantito se sono assicurate le richieste delle schede che seguono:

- La Scheda 3 richiede, per il rispetto del vincolo n.5 del DNSH "*Prevenzione e riduzione dell'inquinamento*", in caso di assenza di etichette ambientali ISO di tipo 1, la certificazione di conformità all'Allegato II della Direttiva RoHS;
- La Scheda 6 richiede, per il rispetto del vincolo n. 5 del DNSH "*Prevenzione e riduzione dell'inquinamento*" che tutte le apparecchiature dei Data Center siano in linea con la Direttiva RoHS. A tal riguardo, è richiesta la Certificazione delle apparecchiature dei DC in conformità con la Direttiva RoHS;
- La Scheda 8 richiede, per il rispetto del vincolo n. 5 del DNSH "*Economia Circolare*", che l'equipaggiamento dei DC non contenga sostanze proibite e nocive in linea con la Direttiva RoHS ed il Regolamento REACH (Regolamento (CE) n.1907/2006 del Parlamento europeo e del Consiglio). In particolare, il regolamento REACH - *Registration, Evaluation, Authorisation and Restriction of Chemicals* – consentirà di verificare la registrazione, valutazione, autorizzazione e restrizione delle sostanze chimiche utilizzate all'interno dei DC, ed inoltre, in relazione al vincolo n. 5 del DNSH "*Prevenzione e riduzione dell'inquinamento*" è richiesta la Certificazione delle apparecchiature dei DC in conformità con la Direttiva RoHS.

Per quanto riguarda la **metodologia di verifica** si presume che le AEE munite di marcatura CE siano conformi alla Direttiva RoHS.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH**, la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di Controllo delle Schede 3, 6 e 8, unitamente all'ottenimento e corretta archiviazione e messa a disposizione di tutta la documentazione richiesta dalla specificità della misura: Certificazione di conformità con la Direttiva RoHS.

#### 1.15.4.9.1 Il rispetto della Direttiva RoHS da parte del RTI – Stato attuale ed azioni future

In conformità alla Direttiva RoHS, tutte le apparecchiature elettriche ed elettroniche che verranno utilizzate nell'ambito del contratto non conterranno le sostanze di cui all'allegato II della medesima Direttiva RoHS in concentrazioni in peso in materiali omogenei superiori ai valori limite ivi riportati. La presente indicazione si riferisce anche ai cavi ed ai pezzi di ricambio destinati alla loro riparazione, al loro riutilizzo, all'aggiornamento delle loro funzionalità o al potenziamento della loro capacità.
Le tipologie di sostanze ricomprese nel perimetro della Direttiva RoHS verranno costantemente monitorate in funzione degli aggiornamenti normativi vigenti.
La conformità alla Direttiva RoHS sarà dimostrata dalla presenza della Marcatura CE su tutte le apparecchiature che verranno utilizzate nell'ambito del contratto.

### *1.15.4.10 Modalità di verifica per accertare che le procedure di approvvigionamento includano la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali; al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della Direttiva 2012/19/UE*

I requisiti prescritti dalla Direttiva 2012/19/UE del Parlamento Europeo e del Consiglio del 4 luglio 2012 sui rifiuti di apparecchiature elettriche ed elettroniche (la "**Direttiva RAEE**") all'interno dell'Allegato VII, prevedono il trattamento selettivo per materiali e componenti di rifiuti di AEE unitamente all'eliminazione di tutti i liquidi.

In relazione al principio del DNSH, in tema di gestione dei beni alla fine del loro ciclo di vita, è necessario rispettare i requisiti descritti nelle Schede 3, 6 e 8:

- Le Schede 3 e 8 richiedono alla Newco, per il rispetto del vincolo n. 4 del DNSH "*Economia Circolare*", l'iscrizione alla piattaforma RAEE in qualità di produttore e/o distributore, come da Decreto Legislativo 14 marzo 2014, n. 49 e ss.mm.ii. ("**D.Lgs. 49/14**") attuativo della Direttiva RAEE.
- Le Schede 6 e 8 richiedono, per il rispetto del vincolo n. 4 del DNSH "*Economia Circolare*", che i DC selezionati abbiano predisposto un piano per lo smaltimento dei rifiuti che permetta di garantire il maggior livello possibile di riciclo, alla fine del ciclo di vita, delle AEE, includendo dei progetti ufficiali e documentati su tale piano ed accordi contrattuali per il corretto riciclo o smaltimento. Alla fine del ciclo di vita delle AEE, esse dovranno essere adeguatamente preparate per il riuso, recupero riciclo o adeguato smaltimento come previsto dalla Direttiva RAEE.

La **metodologia di verifica** si basa sul testo dell'articolo 35 del D.Lgs. 49/14, il quale definisce il soggetto responsabile per la vigilanza ed il controllo nonché i suoi compiti.

Al fine di verificare efficacemente i benefici raggiunti in termini ambientali e per essere *compliant* con la **metodologia di verifica riguardante le prescrizioni del DNSH**, la NewCo metterà a disposizione del Concedente un'autocertificazione, realizzata mediante la compilazione della *Checklist* di Controllo delle Schede 3, 6 e 8, unitamente all'ottenimento e corretta archiviazione di tutta la documentazione richiesta dalla specificità della misura:

- l'iscrizione alla piattaforma RAEE in qualità di produttore e/o distributore;
- adeguata preparazione delle apparecchiature per il riuso, recupero riciclo o adeguato smaltimento come previsto dalla normativa sui RAEE.

#### 1.15.4.10.1 Procedure di trattamento in conformità all'allegato VII della Direttiva RAEE da parte del RTI – Stato attuale ed azioni future

Per quanto riguarda gli aspetti legati all'immissione sul mercato di AEE, Fastweb è iscritta dal 2008 al Registro Produttori di AEE con iscrizione n. IT08020000003838 in relazione alle apparecchiature importate direttamente dall'estero ed alle apparecchiature riportanti il marchio Fastweb. Ai fini dell'applicazione della normativa, Fastweb è, inoltre, iscritta al Consorzio Erion e rinnova annualmente le comunicazioni dovute rispetto ai quantitativi di apparecchiature immesse sul mercato.

Ciò detto, per quanto riguarda il PSN, tutte le apparecchiature elettriche ed elettroniche utilizzate nell'ambito dell'erogazione del servizio verranno gestite in conformità al D.Lgs. 49/14. In particolare, saranno privilegiate le operazioni di riutilizzo e preparazione per il riutilizzo delle apparecchiature, dei loro componenti, sottoinsiemi e materiali di consumo in attuazione dei principi di precauzione e prevenzione, ed al fine di consentire un efficiente utilizzo delle risorse. Le apparecchiature installate presso i DC, che verranno sostituite durante l'erogazione del servizio, verranno ritirate da *System Integrator* specializzati che ne valuteranno la riutilizzabilità in altri ambiti.
In conformità al D.Lgs. 152/06 e ss.mm.ii. ed al D.Lgs. 49/14, laddove non sia possibile un riutilizzo diretto delle apparecchiature ritirate, queste verranno raccolte in modo separato, all'interno di un deposito temporaneo, e da qui avviate ad impianti di recupero specializzati, affinché possano essere recuperati tutti i componenti e i materiali ivi presenti, e possa essere favorito il riutilizzo e il riciclo dei materiali.
Il trasporto dei RAEE verrà affidato esclusivamente a trasportatori autorizzati, iscritti all'Albo Nazionale Gestori ambientali per le tipologie di RAEE conferiti; tali RAEE saranno destinati

esclusivamente a impianti di recupero e trattamento specializzati e in possesso dell'autorizzazione a operare prevista dalla normativa vigente.

## 1.16 ID CRITERIO:16 – VALUTATIVO - MIGLIORAMENTI, A FAVORE DEL CONCEDENTE, DELLA MATRICE DI RIPARTIZIONE DEL RISCHIO. TALI MIGLIORAMENTI, PER ESSERE APPREZZATI, DEVONO ESSERE CHIARI, EVIDENTI E, POSSIBILMENTE, MISURABILI.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 16 | Valutazione | Conduzione | Miglioramenti sugli aspetti ripartizione dei rischi | Miglioramenti, a favore del Concedente, della matrice di ripartizione del rischio. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. | **3** |

L'Offerta, pur accettando *in toto* i contenuti della proposta a base di gara, ivi compresa la Bozza di Convenzione, comprensiva dei suoi allegati e relativo Addendum, propone **un sensibile aumento dei rischi assunti dal Concessionario**, sotto molteplici profili, al fine di migliorare la posizione del Concedente e delle Amministrazioni utenti.
I miglioramenti offerti sono stati concepiti in anche in ossequio alle indicazioni di Eurostat e, in particolare, tenendo conto della guida pubblicata da EPEC, nel 2016, "*A Guide to the Statistical Treatment of PPPs*" (la "**Guida EPEC**"), che illustra nel dettaglio l'applicazione delle previsioni contenute nel "*Manual on Government Deficit and Debt – Implementation of ESA 2010*", pubblicato nel 2016, e, successivamente, aggiornato (ultima versione 2019).
Come previsto dalla direttiva 2014/23/UE (la "**Direttiva Concessioni**"), il contratto di concessione è caratterizzato dal trasferimento, in capo al Concessionario, "*di un rischio operativo legato alla gestione dei lavori o dei servizi, comprendente un rischio sul lato della domanda o sul lato dell'offerta, o entrambi. Si considera che il concessionario assuma il rischio operativo nel caso in cui, in condizioni operative normali, non sia garantito il recupero degli investimenti effettuati o dei costi sostenuti per la gestione dei lavori o dei servizi oggetto della concessione. La parte del rischio trasferita al concessionario comporta una reale esposizione alle fluttuazioni del mercato tale per cui ogni potenziale perdita stimata subita dal concessionario non sia puramente nominale o trascurabile*" (art. 5 della Direttiva Concessioni).
In proposito, le Linee Guida n. 9, recanti «*Monitoraggio delle amministrazioni aggiudicatrici sull'attività dell'operatore economico nei contratti di partenariato pubblico privato* », approvate dal Consiglio dell'Autorità Nazionale anticorruzione con Delibera n. 318 del 28 marzo 2018 - attualmente, soggette a revisione -, (le "**LG PPP**") evidenziano l'importanza della matrice dei rischi come strumento, sia in fase di gara, sia, e soprattutto, in fase di esecuzione contrattuale, per verificare costantemente la corretta allocazione del rischio operativo in capo al concessionario. In tale ottica, le LG PPP precisano che la matrice dei rischi dev'essere costruita in modo da consentire le seguenti funzioni:

1. identificazione del rischio;
2. *risk assessment*, ossia la valutazione della probabilità del verificarsi di un evento associato ad un rischio e dei relativi effetti;
3. *risk management*, ossia l'individuazione dei meccanismi che permettono di minimizzare gli effetti derivanti da un evento;
4. allocazione del rischio al soggetto pubblico e/o privato;

5. corrispondenza tra rischio e trattamento dello stesso all'interno del contratto.

Sulla base delle indicazioni che precedono, la documentazione a base di gara - e, in particolare, la BdC e la matrice dei rischi - allegata *sub* G alla BdC - (la "**Matrice**") evidenziano il trasferimento del rischio operativo sul Concessionario, principalmente:

- in relazione alla progettazione e realizzazione dell'infrastruttura nei tempi e con le caratteristiche indicate, senza alcuna garanzia che il suddetto investimento sia recuperato successivamente mediante la gestione dei relativi servizi;
- sul lato della domanda, in virtù dell'incertezza sul numero di PA che aderiranno al PSN, e sul tipo di servizi (più o meno remunerativi) che richiederanno. Questo rischio è elevato, in considerazione del notevole investimento iniziale richiesto al Concessionario, che potrà essere recuperato solo attraverso i proventi della gestione dei servizi previsti a favore delle PA utenti, Inoltre, questo rischio è sicuramente presente non solo nella fase iniziale della concessione, ossia per tutto il tempo in cui le PA utenti possono, o meno, aderire al PSN, ma anche nella fase a regime, poiché le PA utenti possono decidere di modificare il portafoglio dei servizi richiesti al PSN;
- sul lato dell'offerta/disponibilità e *performance*, in considerazione dell'obbligo, per il Concessionario, di mantenere sempre il livello di qualità dell'infrastruttura e dei servizi richiesto dalla concessione, in conformità agli indicatori previsti, anche mediante le manutenzioni e gli aggiornamenti indicati nei documenti di gara, e dunque, sopportando il rischio di aumento dei costi sottostanti e il relativo rischio tecnologico, senza poter aumentare i propri prezzi (se non nei casi espressamente e tassativamente disciplinati dalla BdC);
- sotto il profilo del rischio finanziario, dovuto alla necessità, per il Concessionario, di assicurarsi i mezzi per poter effettuare gli investimenti e sopportare i costi determinati dall'adempimento degli obblighi contrattuali, senza alcun contributo pubblico da parte del Concedente, ed entro le tempistiche dettate dalla BdC.

Il rischio operativo è, dunque, sicuramente trasferito al Concessionario mediante le previsioni contrattuali.

Peraltro, la BdC a base di gara prevede alcune mitigazioni dei suddetti rischi, al fine di assicurare la sostenibilità della Concessione.

In tale ottica, per evidenziare ed ampliare l'assunzione del rischio operativo in capo al Concessionario, pur preservando l'equilibrio economico-finanziario della Concessione, l'Offerta prevede una significativa riduzione, a favore del Concedente e delle PA, degli elementi di mitigazione del rischio inseriti nella BdC, come illustrato di seguito.

1. Migliorie rispetto al riequilibrio del piano economico-finanziario (art. 11 della BdC):
    a. l'art. 11, comma 4, lett. a della BdC annovera gli eventi di forza maggiore tra quelli che consentono di procedere al riequilibrio. In proposito, l'art. 19, comma 3, della BdC prevede che "*Nel caso di un evento di Forza Maggiore che determini una sospensione del Servizio, parziale, e/o totale per un periodo fino a 30 (trenta) giorni, il Concessionario avrà diritto ad un'automatica proroga del termine di gestione del Servizio per un periodo pari a quello della sospensione. Qualora, invece, la sospensione si protragga per oltre 30 (trenta) giorni e fino ai 180 (centottanta) giorni, il Concessionario potrà anche richiedere la rideterminazione delle condizioni di Equilibrio Economico Finanziario, con le modalità di cui all'art. 11 della Convenzione, qualora ne ricorrano i presupposti.*".
        i. In merito a questa previsione, **si offre di rinunciare alla proroga automatica del termine di gestione del Servizio per i primi 45 giorni di sospensione, nonché di prolungare il periodo di sospensione che non dà luogo al riequilibrio da 30 a 45 giorni**, nella fase di gestione. Tale miglioria non si applica nel periodo di progettazione e realizzazione

dell'infrastruttura, fino all'esito positivo della Verifica di Conformità dell'infrastruttura, di cui all'art. 6, comma 2, lett. b della BdC. Per maggiore chiarezza, a partire dalla fase di gestione, il Concessionario si assumerà il rischio di sospensione a causa di eventi di forza maggiore, senza avere diritto alla proroga automatica, per i primi **45 giorni,** e senza poter accedere al riequilibrio, **per 15 giorni in più**, rispetto a quanto previsto nella BdC. Questa miglioria si pone in linea con quanto previsto nella Guida EPEC, la quale specifica che i rischi derivanti da eventi di forza maggiore sono, generalmente, condivisi, almeno in parte, tra autorità pubblica e *partner* privato, ossia quest'ultimo sopporta una parte delle conseguenze dell'evento (cfr. *Theme* 6.1.3 della guida EPEC);

b. l'art. 11, comma 4, lett. c della BdC prevede, tra gli eventi che consentono di procedere al riequilibrio, "*l'entrata in vigore di norme legislative e regolamentari che incidano sui termini e sulle condizioni di progettazione, predisposizione ed ammodernamento quinquennale dell'infrastruttura nonché di prestazione del Servizio, in particolare, sui costi o i tempi dello stesso, tali da determinare una variazione negativa del TIR del progetto superiore allo 0,15% (zerovirgolaquindici per cento) o la riduzione DSCR minimo ad un livello inferiore a 1.3 X (unovirgolatre)*".
    i. In merito, **si offre un aumento della percentuale di variazione del TIR di progetto che fa scattare il riequilibrio allo 0,17%.** In questo modo, il Concessionario si assume un maggiore rischio di esposizione alle variazioni negative del TIR a causa di modifiche normative pari allo **0,2%**;
c. l'art. 11, comma 5, della BdC prevede che "*Le Parti, fatto salvo quanto previsto ai commi 8 e 10, convengono di procedere alla revisione del PEF contrattuale e della Convenzione, oltre che al verificarsi di una Variazione dell'Equilibrio dovuta a una delle fattispecie di cui al comma 4, anche laddove, al trentesimo (30°) mese dalla stipula della presente Convenzione, per effetto di un evento non imputabile al Concessionario la Variazione dell'Equilibrio determini un TIR di progetto, al netto delle imposte, inferiore al 2,4% (duevirgolaquattro per cento)*".
    i. In merito, **si offre un livello del TIR di progetto che consente di attivare questa ipotesi di riequilibrio al 2,2% (due virgola due per cento)** (anziché il 2,4%). Questa miglioria consente di trasferire un maggiore rischio sul Concessionario, quantificabile in **0,2 punti percentuali** del TIR di progetto;

2. **Migliorie rispetto alle clausole di "*profit sharing*" (art. 10 della BdC):**
    a. l'art. 10, comma 1, della BdC prevede che "*A partire dalla Data di Decorrenza del Periodo di Verifica dell'Andamento Commerciale della Concessione, qualora per effetto di una adesione al* PSN *superiore a quella prevista ai sensi del PEF, i ricavi effettivamente percepiti dal Concessionario al netto dei costi effettivamente sostenuti, comprensivi di imposte e detrazioni dovute ad ogni titolo, presenti e future dovessero determinare un incremento del TIR di Progetto in misura superiore del 2% (due per cento) rispetto al livello previsto nel PEF quale indicatore dell'Equilibrio Economico Finanziario (la "Soglia Rilevante di Incremento del Rendimento del TIR di Progetto"), il Concessionario rimodulerà per il periodo rimanente i prezzi in modo da retrocedere al Concedente e/o alla Amministrazione utente la quota parte di beneficio eccedente la Soglia Rilevante di Incremento del Rendimento, fermo restando l'Equilibrio Economico Finanziario come di tempo in tempo aggiornato*".
        i. In merito, **si offre di abbassare la "*Soglia Rilevante di Incremento del Rendimento del TIR di Progetto*" all'1,8% (uno virgola ottanta per cento)**. In tal modo, il Concessionario sarà tenuto a rinunciare a una percentuale

più alta dello **0,2%** del proprio beneficio, a favore del Concedente e delle PA utenti;

b. l'art. 10, comma 3, terzo alinea della BdC prevede, in caso di rifinanziamento, che "*Qualora il Rifinanziamento comporti dei benefici per il Concessionario tali da determinare un incremento del TIR dell'Equity in misura superiore del 2% (due per cento) rispetto al livello previsto nel PEF quale indicatore dell'Equilibrio Economico Finanziario, verificati attraverso l'inserimento delle opportune modifiche nel Piano Economico Finanziario contrattuale (il "Beneficio da Rifinanziamento"), detto Beneficio da Rifinanziamento calcolato dal Concessionario e comunicato al Concedente e sarà condiviso con il Concedente in misura pari a un massimo del 33% (trentatrè per cento)*".
   i. In merito, **si offre di ridurre la soglia di incremento del TIR dell'*equity* che costituisce il "*Beneficio da Rifinanziamento*" all'1,8% (uno virgola ottanta per cento),** in tal modo, aumentando dello **0,2%** la propria rinuncia al suddetto "*Beneficio da Rifinanziamento*", in favore del Concedente e delle PA utenti;

3. **Migliorie relative alla devoluzione dell'Infrastruttura (art. 38 della BdC):**
   a. l'art. 38, comma 2 della BdC prevede che "*Per la devoluzione dell'infrastruttura, al Concessionario sarà dovuto un rimborso pari al valore residuo dell'infrastruttura stessa, al netto dell'ammortamento degli investimenti intervenuto in ragione dell'esercizio delle attività di concessione, per come desumibile dal bilancio del Concessionario, tenendo anche conto dell'obsolescenza tecnologica a cui la stessa è soggetta valutata dal Comitato di Controllo di cui all'articolo 12 che, per tale attività, può avvalersi anche della collaborazione di esperti in possesso di specifica ed elevata competenza in materia tecnico informatica*".
      i. In merito, si offre che il rimborso per la devoluzione sia pari al 90% (novantapercento) del valore residuo **dell'Infrastruttura,** In tal modo, assumendo un rischio pari al 10% (diecipercento) del valore residuo dell'Infrastruttura.

Dal complesso delle migliorie offerte, emerge un profilo di rischio operativo molto più spinto, rispetto a quello posto a base di gara. Si tratta, peraltro, di migliorie volte a favorire il Concedente e le PA utenti, ma che non minano la solidità del piano economico-finanziario dell'Offerta, mantenendone l'equilibrio.

Per completezza, si riporta di seguito **la nuova Matrice dei Rischi proposta dall'Offerente**, con evidenziate in rosso le migliorie rispetto alla versione presente nella Documentazione di Gara.

*Tabella 9: Nuova Matrice dei Rischi proposta dall'Offerente - migliorie in rosso*

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di progettazione e predisposizione ed allestimento** | Rischio derivante da errori od omissioni di progettazione, predisposizione ed allestimento dei locali attrezzati funzionali alla fornitura dei servizi, in relazione alle variabili tecnologiche ed operative | Alta | Ritardi nell'avvio della fase operativa del progetto e/o Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR. RISCHIO AUMENTATO IN VIRTÙ DEL TERMINE INFERIORE OFFERTO DI 120 GIORNI (Cfr. Relazione ID.CRITERIO 10) | Contratti di "costruzione" con previsione di garanzie contrattuali e clausole tipiche. | | ✓ | **Art. 5; Art. 6; Art. 8, comma 3, lett. f); Art. 11; Art. 14; Art. 19; Art. 21; Art. 22; Art. 26; Art. 27; Art. 33, comma 2, lett. a) e c); Art. 39.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di domanda** | Rischio di domanda relativo al numero di Amministrazioni utenti che decideranno di migrare nonché alla quantità e tipologia di servizi che le stesse richiederanno | Alta | Diminuzione dei ricavi e dei costi parametrati ai volumi. Contestuale riduzione del MOL, dell'utile netto e del TIR. | Obbligo per le PA di rimborsare il PSN dei costi sostenuti ed eventualmente corrispondere una fee a parziale copertura dei mancati ricavi In caso di early termination. Riequilibrio del PEF in caso di rendimento inferiori alla soglia individuata. SOGLIA DEL TIR DI PROGETTO RIDOTTA AL 2,2% NEL CASO DI CUI ALL'ART. 11, COMMA 5 (cfr. Relazione ID.CRITERIO 16). | ✓ | ✓ | **Art. 5; Art. 9, comma 1, lett. a); Art. 10; Art. 11.** |
| **Rischio di gestione** | Rischio dei ricavi derivante da una errata valutazione delle tariffe applicate | Bassa | Diminuzione dei ricavi con contestuale riduzione del MOL, dell'utile netto e del TIR. RISCHIO AUMENTATO IN VIRTÙ DEL MECCANISMO DI SCONTO GARANTITO PER LA REVISIONE PREZZI EX ART. 5, COMMA 4, PUNTO iii DELLA BOZZA DI CONVENZIONE (Cfr. Relazione ID.CRITERIO 18) | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✓ | **Art. 5; Art. 9, comma 1, lett. c); Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 26; Art. 33, comma 2, lett. a), c); Art. 39.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di Gestione** | Incremento dei costi di fornitura dei servizi affidati al concessionario | Alta | Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✓ | **Art. 5; Art. 9, comma 1, lett. c); Art. 11; Art. 14; Art. 19; Art. 20; Art. 26; Art. 33, comma 2, lett. a), c); Art. 39.** |
| **Rischi di investimento** | Rischi di investimento legati all'approvvigionamento ed ai costi delle componenti degli impianti tecnologici infrastrutturali dei Data Center funzionali alla fornitura del servizio | Alta | Aumento dei capex e dell'ammortamento relativo, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di approvvigionamento standard con previsione di garanzie contrattuali e clausole tipiche. | | ✓ | **Art. 5; Art. 9, comma 1, lett. d); Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 33, comma 2, lett. c).** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di disponibilità** | Rischio di aumento dei costi di manutenzione ordinaria e di manutenzione straordinaria non preventivata o maggiore rispetto a quanto previsto nel PEF | Alta | Aumento dei costi operativi, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✓ | **Art. 5; Art. 8, comma 3, lett. b); Art. 9; Art. 10; Art. 12; Art. 14; Art. 20; Art. 21; Art. 22; Art. 38.** |
| **Rischio di disponibilità** | Mancato rispetto degli standard prestazionali - sia qualitativi che quantitativi - rilevato attraverso gli organismi e meccanismi preposti al controllo, con applicazioni di penali differenziate in ragione del servizio e dell'entità della violazione | Bassa | Aumento dei costi straordinari relativi alle penali, con contestuale riduzione del MOL, dell'utile netto e del TIR. RISCHIO AUMENTATO IN VIRTÙ DELLE MIGLIORIE APPORTATE IN RELAZIONE AGLI indicatori di qualità IQ11, IQ12, IQ13 E IQ14 (cfr. Relazione ID.CRITERIO 8) | Contratti con definizioni di penali e rimborsi limitati a un tetto massimo standard. | | ✓ | **Art. 5; Art. 9, comma 1, lett. b); Art. 10; Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 23; Art. 39.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischi finanziari** | Rischi finanziari relativi al mancato reperimento delle risorse di finanziamento a copertura dei costi e nei tempi prestabiliti ed all'oscillazione dei tassi di interesse | Bassa | Potenziale aumento degli oneri finanziari con contestuale diminuzione dell'utile netto e del TIR.<br>RIFINANZIAMENTO:<br>• ABBASSAMENTO DELLA "SOGLIA RILEVANTE DI INCREMENTO DEL RENDIMENTO DEL TIR DI PROGETTO" ALL'1,8%<br>• RIDUZIONE DELLA SOGLIA DI INCREMENTO DEL TIR DELL'EQUITY CHE COSTITUISCE IL "BENEFICIO DA RIFINANZIAMENTO" ALL'1,8%<br>(cfr. Relazione ID.CRITERIO 16) | | | ✓ | **Art. 9, comma 1, lett. e);<br>Art. 28<br>Art. 32<br><br>Art. 10, comma 1 e comma 3** |
| **Forza Maggiore** | Forza maggiore che comporti modifica del Piano Economico-Finanziario. | Minima | SOSPENSIONE DEL SERVIZIO FINO A 45 GIORNI SENZA DIRITTO AD ALCUNA PROROGA DELLA DURATA CONTRATTUALE.<br>SOSPENSIONE DEL SERVIZIO SENZA DIRITTO AD ALCUN RIEQUILIBRIO DEL PEF FINO A 45 GIORNI.<br>(cfr. Relazione ID.CRITERIO 16)<br>Riallineamento del PEF e potenziale chiusura della concessione, con | SOLO DOPO 45 GIORNI<br>Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✓ | | **Art. 11;<br>Art. 19;<br>Art. 37.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | | | eventuale implementazione di un termination payment. | | | | |
| **Mutamenti imposti ex lege** | Mutamenti imposti ex lege (ivi compresi mutamenti relativi ad innovazioni tecnologiche, strumenti e/o tecniche diverse) che comportino modifica del PEF | Media | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. RISCHIO AUMENTATO IN VIRTÙ DELL'INNALZAMENTO DELLA PERCENTUALE DI VARIAZIONE DEL TIR DI PROGETTO CHE FA SCATTARE IL RIEQUILIBRIO ALLO 0,17% (cfr. Relazione ID.CRITERIO 16) Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✓ | ✓ | **Art. 5; Art. 11; Art. 37.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Mutamenti richiesti dal Concedente** | Mutamenti richiesti dal Concedente (es. relativi ad innovazioni tecnologiche) | Molto alta | Riallineamento del PEF. | | ✓ | | **Art. 5; Art. 11; Art. 37** |
| **Danni subiti dal Concedente e da terzi** | Danni subiti dal Concedente e da terzi riconducibili all'espletamento dei servizi, e per tutta la durata della concessione (ex art. 1891) | Bassa | Aumento dei costi straordinari per eventuali rimborsi del danno. | Contratti con clausole limite in caso di rimborso del danno. | | ✓ | **Art. 27 Art. 33, comma 2, lett. d)** |
| **RISCHIO DI VALORE RESIDUO AL TERMINE DELLA CONCESSIONE** | RISCHIO DI CESSIONE DI BENI NON ANCORA AMMORTIZZATI | MEDIA | RIMBORSO PER LA DEVOLUZIONE PARI AL 90% VALORE RESIDUO DELL'INFRASTRUTTURA (cfr. Relazione ID.CRITERIO 16) | | | ✓ | **Art. 38** |

## 1.17 ID CRITERIO:17 – VALUTATIVO - MIGLIORAMENTI DEL MODELLO DI GOVERNANCE UTILI A CONSENTIRE UN MAGGIOR COINVOLGIMENTO DEL CONCEDENTE ANCHE NELL'OTTICA DI GARANTIRE ULTERIORMENTE LA VIGILANZA E IL MONITORAGGIO PUBBLICO. TALI MIGLIORAMENTI, PER ESSERE APPREZZATI, DEVONO ESSERE CHIARI, EVIDENTI E, POSSIBILMENTE, MISURABILI.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 17 | Valutazione | Conduzione | Miglioramenti sugli aspetti governance | Miglioramenti del modello di governance utili a consentire un maggior coinvolgimento del Concedente anche nell'ottica di garantire ulteriormente la vigilanza e monitoraggio pubblico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. | **4** |

L'Offerta accetta *in toto* i contenuti della proposta a base di gara, ivi compresa la Bozza di Convenzione, comprensiva dei suoi allegati e relativo Addendum.

Di seguito vengono illustrati i miglioramenti sugli aspetti di *governance* sia societaria-amministrativa che tecnologico-operativa.

### 1.17.1 Miglioramento su *governance* societaria ed amministrativa

Con riferimento agli aspetti di *governance* amministrativa e societaria, l'Offerta propone miglioramenti chiari, evidenti e misurabili, delineati sull'organizzazione societaria della NewCo e sulla base del complesso di norme in materia di poteri speciali sugli assetti societari esercitabili dal Governo in determinati ambiti di rilevanza strategica - cd. "*Golden Power*" (il "GP") -, che, secondo la *lex specialis* di Gara, trovano applicazione alla NewCo.

#### *1.17.1.1 Miglioramento in merito agli organi statutari della NewCo ed ai rapporti con il Concedente*

A pag. 25 del Progetto di fattibilità posto a base di gara, è previsto che "*La NewCo avrà ovviamente un proprio Amministratore Delegato ed un Presidente*".

In merito, si offre di inserire altresì espresse previsioni statutarie della NewCo con le quali:

a. è previsto, quale organo della NewCo, un Consiglio di Amministrazione composto da 7 membri.
   Si offre al Concedente il diritto di indicare un membro del Consiglio di Amministrazione. L'eventuale indicazione da parte del Concedente sarà vincolante per il Concessionario ed i suoi soci.
   Il Consiglio di Amministrazione è l'organo deputato alla gestione della società per azioni, fatta salva la delega dei poteri a favore dell'Amministratore Delegato. Delibera in merito alle operazioni della società che hanno un significativo rilievo strategico, economico, patrimoniale o finanziario per la società stessa. Pertanto, la scelta di riservare il ruolo di uno

dei componenti il Consiglio di Amministrazione ad un soggetto individuato dal Concedente rafforza, in modo concreto e stabile, la funzione di vigilanza e monitoraggio pubblico che assume un ruolo incisivo nell'esecuzione della Convenzione.

b. è previsto, quale organo di controllo, un Collegio sindacale composto da 5 membri effettivi, oltre a due sindaci supplenti.
**Si offre al Concedente il diritto di indicare un membro del Collegio sindacale. L'eventuale indicazione da parte del Concedente sarà vincolante per il Concessionario ed i suoi soci.**
Il Collegio sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e, in particolare, sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento.
I sindaci, inoltre, possono in qualsiasi momento procedere, anche individualmente, ad atti di ispezione e di controllo. Il Collegio sindacale può chiedere agli amministratori notizie sull'andamento delle operazioni sociali, o su determinati affari. I sindaci devono, inoltre, assistere alle adunanze del Consiglio di Amministrazione, alle assemblee.
L'attribuzione del ruolo di sindaco effettivo in capo ad un professionista individuato dal Concedente rappresenta un ulteriore ampliamento del potere di controllo e monitoraggio sull'andamento della NewCo, sulla corretta esecuzione della concessione e sull'andamento del piano economico finanziario in un'ottica di piena trasparenza e correttezza della gestione.

c. Inoltre, si offre un impegno da parte delle imprese facenti parte dell'Offerente, anche quali future socie della costituenda NewCo, **a consentire l'ingresso all'interno della compagine societaria della NewCo di un soggetto pubblico o a partecipazione pubblica, indicato dal Concedente**, quale socio di minoranza con quota fino al 15% del capitale sociale che, sulla base dei desiderata del Concedente e verificato il possesso dei requisiti da parte della stessa Concedente, potrà assumere il ruolo di socio.

#### *1.17.1.2 Miglioramento in merito alla disciplina del Golden Power (GP)*

Il GP, come noto, è stato introdotto nel nostro ordinamento con il d.l. n. 21 del 2012, convertito con la legge n. 56 del 2012 e ss.mm.ii. (il "**DL 21/12**"), relativa ai "*poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni*".

Il DL 21/12 (art.1), in relazione al settore della difesa e della sicurezza nazionale, attribuisce al Governo i seguenti poteri:

a. imposizione di specifiche condizioni relative alla sicurezza degli approvvigionamenti e delle informazioni, ai trasferimenti tecnologici, al controllo delle esportazioni nel caso di acquisto, a qualsiasi titolo, di partecipazioni in imprese che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale;
b. veto all'adozione di determinate delibere dell'assemblea o degli organi di amministrazione di un'impresa strategica, concernenti segnatamente: (**i**) la fusione o la scissione della società; (**ii**) il trasferimento dell'azienda o di rami di essa o di società controllate; (**iii**) il trasferimento all'estero della sede sociale; (**iv**) il mutamento dell'oggetto sociale; (**v**) lo scioglimento della società; (**vi**) la modifica di clausole statutarie eventualmente adottate ai sensi dell'art. 2351 comma 3 c.c. 1, ovvero introdotte ai sensi dell'art. 3, comma 1 d.l. 332/1994; (**vii**) le cessioni di diritti reali, o di utilizzo, relative a beni materiali o immateriali o l'assunzione di vincoli che ne condizionino l'impiego;
c. opposizione all'acquisto di partecipazioni, in imprese strategiche, da parte di soggetti diversi dallo Stato, dagli enti pubblici italiani o da questi controllati, qualora l'acquirente possa detenere, direttamente o indirettamente, "*un livello della partecipazione al capitale con diritto*

*di voto in grado di compromettere nel caso specifico gli interessi della difesa e della sicurezza nazionale*.".

L'art. 2 del DL 21/12 riconosce al Governo, in relazione alle imprese strategiche - operanti nei settori dell'energia, dei trasporti e delle comunicazioni-, oltre ai poteri di cui all'art. 1, dei poteri speciali riguardanti sia determinate operazioni societarie, sia il trasferimento di partecipazioni di controllo in tali società.
In particolare, in merito a:

a. le operazioni societarie - il Governo può opporre il veto su qualsiasi "*delibera, atto o operazione*", consistente nella modifica della titolarità, del controllo o della disponibilità di attivi, ovvero il cambiamento della loro destinazione;
b. il trasferimento delle partecipazioni societarie - il Governo può sia condizionare l'efficacia dell'acquisto di una partecipazione di controllo - da parte di un soggetto esterno all'UE - all'assunzione di impegni diretti a garantire la tutela di interessi essenziali dello Stato, sia opporsi all'acquisto medesimo, in casi eccezionali di rischio per gli stessi interessi.

*****

In linea con la normativa sopra illustrata, si evidenziano i chiari ed evidenti miglioramenti del modello di *governance*, oggetto dell'Offerta, volti a consentire un maggior coinvolgimento del Concedente ed una maggiore vigilanza e monitoraggio pubblico, pur preservando la corretta attribuzione delle responsabilità contrattuali e dei rischi in capo al Concessionario.

*****

Tali migliorie costituiscono un avanzamento anche rispetto a quanto previsto nella BdC, in particolare all'art. 7 della stessa, il quale prevede che "*L'ingresso di nuovi soci nel capitale del Concessionario che non siano investitori istituzionali, incluso quello derivante dalla cessione di partecipazioni da parte dei soci qualificanti in aggiunta a quelli che hanno concorso a formare i requisiti per la qualificazione, è subordinato, a pena di risoluzione per inadempimento del Concessionario ai sensi dell'articolo 33 della Convenzione, al consenso del Concedente.*
*Di tutte le variazioni nel capitale sociale della Concessionaria, quest'ultima si impegna ad informare tempestivamente il Concedente che, ove richiesto, si obbliga a rilasciare il relativo consenso entro 30 giorni dal ricevimento della richiesta da parte della Concessionaria restando inteso che, a termini dell'art. 20 della l. 7 agosto 1990, n. 241, decorso detto termine senza che sia pervenuto il diniego del consenso del Concedente, la modifica della compagine societaria si intende accettata e diviene pertanto efficace.*"

Ferma restando, dunque, la piena applicazione alla NewCo sia delle disposizioni sul GP, sia della previsione della BdC sopra riportata, si offre di inserire una previsione statutaria della NewCo con la quale verrà riconosciuta in capo al Concedente un'estensione dei diritti di veto già previsti dalle suddette disposizioni, rendendoli applicabili anche in merito all'adozione di delibere assembleari e/o consiliari aventi ad oggetto:

a. l'acquisizione, da parte della NewCo, di partecipazioni in società;
b. il trasferimento della sede sociale anche all'interno del territorio Italiano, oltre che in Paesi esteri;
c. la costituzione (in Italia o in Paesi esteri) di società;
d. la modifica delle clausole statutarie e/o l'introduzione o modifica dei patti parasociali che incidano sul ruolo di vigilanza e monitoraggio in capo al Concedente;
e. l'acquisizione di *asset* strategici o comunque di valore superiore a Euro 1.000.000;
f. la costituzione di pegno sulle azioni.

Inoltre, **si offre l'impegno a rendere una costante e compiuta informativa** a favore del Concedente avente ad oggetto **il trasferimento della proprietà dei beni aziendali di rilievo strategico o di valore superiore a Euro 1.000.000**.

### 1.17.2 Miglioramenti operativi e tecnologici

A pag. 22 del Progetto di fattibilità posto a base di gara è previsto che "*All'Organizzazione di Sicurezza saranno attribuiti compiti di controllo e supervisione in relazione alla corretta implementazione nei vari ambiti operativi. Il Responsabile di tale organizzazione potrà essere individuato in accordo con le autorità istituzionali competenti e sarà dotato di specifici requisiti (es. NOS, cittadinanza italiana).*"

L'Offerente, nel confermare l'accettazione *in toto* anche di detta previsione relativa al Responsabile dell'Organizzazione di Sicurezza, intende proporre modalità ulteriormente migliorative di gestione operativa, volte a garantire un maggior coinvolgimento del Concedente, assicurando una maggiore vigilanza e un monitoraggio pubblico più capillare sulla gestione delle attività del PSN.

A tal fine, l'Offerente propone una serie di **evoluzioni operative e tecnologiche,** che migliorano significativamente il modello di *governance* operativo e tecnologico nel suo complesso.

Questi miglioramenti, descritti nel dettaglio nei paragrafi successivi, si basano su:

1.1 Creazione di una **struttura organizzativa di *Governance***, con specifici obiettivi di controllo e sorveglianza e un ruolo più chiaro nel rapporto con il Concedente e gli altri Enti preposti, per consentire a questi ultimi di esercitare poteri di indirizzo e di controllo sul PSN;
1.2 Integrazione dei **soggetti nominati dal Concessionario**, previsti all'art. 13 della BdC, con un referente specifico per la sicurezza informatica;
1.3 Migliorie in **ambito monitoraggio e *reporting***, a beneficio della completezza e trasparenza delle informazioni che saranno rese disponibili al Concedente ed alle PA utenti, attraverso i seguenti strumenti:
   a. adozione di un processo di ***Quality Assurance***, volto a migliorare il monitoraggio ed il *reporting* verso il Concedente e le PA utenti in ottica di *continuous improvement*;
   b. adozione di strumenti di ***Cloud Financial Management***, per un maggior controllo e trasparenza dei costi;
   c. **evoluzione** di quanto previsto in ambito monitoraggio e *reporting* sulle varie componenti oggetto di monitoraggio (ad es. *hardware*, sistemi, *performance*, *ticket*, costi), con particolare riferimento all'adozione di ***monitoring* proattivo e predittivo** supportato da **strumenti tecnologici all'avanguardia, quali il *Machine Learning***.

#### *1.17.2.1 Struttura organizzativa di Governance*

L'Offerente, nell'ottica di migliorare il modello di *Governance* del PSN, propone alcune migliorie che vanno a rafforzare la ***Governance*** - fermo restando quanto previsto nella documentazione di gara, in particolare nel Progetto di fattibilità, par 1.5.1 e nel Capitolato servizi, par. 2.6 e 2.8 -, con riferimento alle responsabilità di controllo e sorveglianza del PSN ed agli obblighi in tal senso del Concessionario nei confronti del Concedente, degli altri Enti preposti e delle PA utenti.

L'Offerente propone di definire una specifica **struttura organizzativa per la *Governance* del PSN, con personale, chiaramente identificato,** che adotterà processi e strumenti in linea con i modelli più avanzati di governo delle infrastrutture IT e sistemi *cloud*.

Le principali funzioni di controllo e sorveglianza in carico alla struttura di *Governance* saranno:

- controllo dell'**interoperabilità** e della ***compliance***, anche attraverso funzioni di verifica ed a*udit* interni, in grado di fornire i relativi dati alle autorità, alle PA utenti ed agli Enti preposti al controllo ed al monitoraggio del PSN;
- controllo e **gestione dei costi** in relazione ai Contratti di utenza sottoscritti dalle singole PA;
- **controllo dell'esercizio** dei servizi del PSN, con processi di contatto chiari, "*focal point*" dedicati e procedure di rapporto formalizzate;
- **controllo dei Livelli di Servizio** del PSN, con strumenti di definizione, monitoraggio e verifica dei Livelli di Servizio relativi alla Concessione e specifici per ogni PA utente;
- pianificazione del **percorso di evoluzione della gamma dei Servizi PSN disponibili**, condivisa e costantemente aggiornata con le **PA utenti** e gli **Enti preposti**;
- governo delle architetture infrastrutturali ed applicative attraverso funzioni di "***Design Authority***";
- condivisione dei **piani formativi** che saranno erogati alle PA utenti, al fine di validare e indirizzare al meglio il percorso delle stesse PA utenti verso il *cloud*;
- sorveglianza della ***cybersecurity***, con modalità in grado di consentire il controllo e il monitoraggio puntuale da parte del Concedente e degli Enti preposti e delle PA utenti.

Nell'ambito della *cybersecurity* saranno, in particolare, predisposte funzioni di ***Security Governance*** e ***Reporting***, orientate alla definizione delle regole di sicurezza da applicare al PSN sulla base dei requisiti normativi, della valutazione e gestione dei rischi, nonché delle esigenze specifiche delle PA utenti. Tali funzioni, inoltre, avranno in carico le attività di ***assessment*** **sui dati delle PA utenti** per la loro classificazione (strategici, critici, ordinari), che saranno **condivise con il Concedente,** al fine di garantire vigilanza e monitoraggio pubblico.
In questo ambito, saranno anche erogate le attività di monitoraggio dei Livelli di Servizio di sicurezza, compresa la condivisione periodica con le PA utenti degli indicatori rilevanti dal punto di vista della sicurezza logica e fisica e della conformità ai requisiti di legge.
Il raggiungimento dei Livelli di Servizio sarà costantemente monitorato ed oggetto di specifici rapporti con periodicità trimestrale.

La struttura di *governance* svolgerà le sue funzioni su due livelli:

- verso **il Concedente e gli altri Enti preposti, per consentire a questi ultimi di esercitare il proprio controllo ed i poteri di indirizzo sul PSN**;
- verso le **PA utenti**, per facilitare l'accesso ai **Servizi PSN, accompagnando le PA utenti in tutto il percorso - ossia, dalla valutazione preliminare all'esercizio** - e **per esercitare il proprio controllo ed i poteri di indirizzo, sui servizi in ambito dei Contratti di utenza**.

Sarà, inoltre, responsabilità della struttura operativa di *Governance* garantire, anche a livello societario, tutti i necessari accorgimenti per garantire la rispondenza ai **criteri di sicurezza, tutela e nazionalità dei dati**.

#### *1.17.2.2* Integrazione dei soggetti nominati dal concessionario

Fermo restando quanto previsto dall'art.13 della BdC ("*SOGGETTI NOMINATI DAL CONCESSIONARIO*"), l'Offerente propone di aggiungere alle figure previste nella BdC (Direttore del Servizio, Referente del Servizio) un referente specifico per i temi di *Cyber Security*. Si propone, quindi, di aggiungere al citato art. 13 la previsione che segue:

*"Sempre entro 20 (venti) giorni dalla sottoscrizione della Convenzione, il Concessionario nomina e comunica al MITD un soggetto adeguatamente qualificato come Referente della Cybersecurity, con il compito di gestire i rapporti con il DEC del MITD e/o della singola Amministrazione utente, per gli aspetti riguardanti le tematiche di Sicurezza Informatica.*

#### *1.17.2.3 Ambito Monitoraggio e Reporting*

##### 1.17.2.3.1 *Quality Assurance*

Ad integrazione di quanto previsto nell'ambito della struttura operativa di *Governance*, l'Offerente propone di dotare la NewCo di un processo strutturato e ruoli di *Quality Assurance*, per controllare, in maniera proattiva, la qualità dei servizi resi, assicurando la misura delle *performance* e lo stato dei processi, l'identificazione delle differenze rispetto alle aspettative ed ai *target* operativi definiti, da gestire in ottica di *service improvement*.

Le responsabilità in ambito *Quality Assurance* saranno chiaramente identificate all'interno della NewCo. In particolare, saranno identificate delle figure di *Quality Lead* all'interno delle varie strutture, in carico della *Quality Assurance* interna alla struttura stessa, coordinate centralmente dalla struttura operativa di *Governance,* che ne assume in questo modo la responsabilità finale.

Strumenti essenziali per il processo di *Quality Assurance* sono i controlli permanenti, eseguiti con cadenza periodica. Nel caso in cui fossero evidenziate eventuali aree di minore copertura, queste saranno prontamente indirizzate da azioni, secondo un programma strategico di *continuous improvement*. Le attività di controllo sono di natura periodica, classificate in:

- controlli formali: riguardano l'analisi e la valutazione dei risultati prodotti dall'inizio del contratto, siano essi intermedi o finali, con l'obiettivo di verificare la presenza di tutti gli *output* previsti e la loro conformità agli *standard* fissati, valutandone eventuali scostamenti, indicandone cause, possibili impatti ed eventuali azioni da intraprendere per il trattamento delle non conformità. Sono oggetto di controllo formale non solo tutti i prodotti intermedi e finali del progetto, ma anche i documenti relativi alla gestione del progetto stesso;
- controlli sostanziali: fissano l'attenzione sul contenuto e la congruità dei risultati, siano essi intermedi o finali, in forma documentale o di moduli *software*, con l'obiettivo di verificare che il risultato esaminato sia congruente con i requisiti e con i vincoli fissati per il prodotto, valutandone eventuali scostamenti, indicandone cause, possibili impatti ed azioni da intraprendere per il trattamento delle non conformità. Saranno coinvolti in questa fase di revisione anche esperti dello specifico dell'ambiente tecnologico utilizzato o dominio di *software* di base o applicativo, se applicabile;
- controllo dello stato avanzamento lavori;
- validazione dei risultati.

Le aree soggette a monitoraggio permanente saranno, almeno, le seguenti:

- *Hardware Monitoring* (verifica funzionalità, *performance* e carico CPU, spazio disco, controllo stato ed allocazione di memoria, controllo dei processi e delle priorità di esecuzione, monitoraggio dei sistemi di I/O, controllo delle prestazioni di rete e monitoraggio della connettività);
- *Storage Monitoring*;
- *Software Monitoring* (Sistemi Operativi, *server database*, *file system*, controllo e gestione dei *log* di sistema, piano di licenze);
- *Middleware Monitoring*;
- *Backup Monitoring*;

- *Database Monitoring;*
- *VMware Host Monitoring*;
- *Performance Monitoring* (CPU, RAM, I/O, etc;)
- *Security Monitoring*, che include:
    - Controlli di *hardening* dei *server*;
    - Controlli di corretta esecuzione dei processi di *integrity patching*;
    - Controlli di corretta esecuzione dei processi di *remediation*, a fronte di rilevazione di vulnerabilità;
    - Controlli di corretta esecuzione dei processi di ri-validazione delle utenze privilegiate.

#### 1.17.2.3.2 *Cloud Financial Management*

Al fine di garantire trasparenza e visibilità sulla spesa e di fornire accesso allo storico dei costi, con la possibilità di analizzarne i *trend* e di consentirne una previsione nel breve-medio termine, l'Offerente propone l'adozione di un *tool* di *Cloud Financial Management*, che fornisce visibilità granulare di tutti gli ambienti *cloud*, analizzando lo *spending* per dipartimenti, *team*, progetti o applicativi. L'analisi dei costi può supportare valutazioni di revisione architetturale di determinati servizi, conveniente per un miglioramento delle *performance* e contemporanea ottimizzazione dei costi.
I principali vantaggi derivanti dall'implementazione della soluzione di *Cloud Financial Management* sono:

- Ottimizzazione dei costi *cloud*:
    - utilizzo delle funzionalità di modellazione, ottimizzazione e ammortizzazione incluse nel *tool* stesso, che riducono la necessità di attività manuali;
    - identificazione di opportunità di risparmio valutando l'effettivo utilizzo delle risorse e selezionando i piani e le scontistiche offerti dai *Cloud provider* (per esempio, acquisto di *reserved instances* nel caso di *workload* stabili nel tempo) in linea con le esigenze di *business*.
- Gestione dello *spending* per linee di *business*:
    - garanzia che le linee di *business* siano conformi con le linee guida in termini di *budget*, tramite un sistema proattivo di monitoraggio, controllo e notifica dello *spending*, valutato rispetto a *target* pre-impostati. È possibile attivare una serie di pratiche automatiche di *cost-saving*, tramite la definizione di *policy* che monitorano costantemente eventuali opportunità di riduzione di inefficienze.
- Formazione/diffusione di una cultura di *accountability* finanziaria:
    - allineamento dei dati finanziari relativi al *cloud* rispetto a metriche di riferimento per il *business*, quali il *gross margin* ed il *cost of goods sold*, per una convergenza degli obiettivi dell'intera organizzazione.

Di seguito, si riporta un esempio di *report* generato dal *tool* di *Cloud Financial Management*:




*Figura 28: Dashboard di costi cloud per servizio ed elemento infrastrutturale*

#### 1.17.2.3.3 *Evoluzioni in ambito monitoring e reporting*

Le evoluzioni in ambito *monitoring* e *reporting* saranno abilitate mediante l'adozione di opportune procedure supportate da componenti tecnologiche quali:

- Un **CMDB** (*Configuration Management Data Base*) accurato, completo, coerente, affidabile, che sia costantemente alimentato ed aggiornato grazie all'utilizzo di *tool* di *Asset Discovery*. Il CMDB, così popolato, supporterà l'identificazione e la definizione del perimetro oggetto del monitoraggio;
- ***Data Analytics*** e ***Machine Learning*** per la correlazione delle informazioni.

Tali evoluzioni consentiranno l'erogazione dei seguenti servizi evoluti:

1. Monitoraggio hardware

Il servizio di monitoraggio *Hardware* si focalizza prevalentemente sui *server* gestiti in modalità *Housing* ed include le seguenti aree:

- **Monitoraggio degli eventi**: gli eventi sono rilevati e monitorati tramite agenti installati sui sistemi di interesse; al verificarsi di un evento significativo, il sistema di automazione interviene, eseguendo le azioni e generando le notifiche *real-time* previste per il caso specifico. I dati raccolti dal sistema di automazione vengono convogliati al sistema di analisi e *reporting*, per l'esecuzione di analisi retrospettive e per la creazione di *dashboard* statiche e dinamiche.
- **Monitoraggio della disponibilità**: il livello di disponibilità infrastrutturale viene mantenuto sotto controllo presidiando i parametri di tempo medio di risoluzione degli *incident* (MTTR) e l'intervallo medio di occorrenza degli *incident* (MTTF); è prevista l'attivazione di un sistema di notifica automatico che segnali una situazione potenzialmente critica, rispetto a livelli *target* attesi e definiti con la PA dei due parametri su intervalli temporali significativi. Analizzando i dati raccolti a seguito del monitoraggio, si ottengono evidenze quali l'impatto generato dalla numerosità degli *incident* e quello generato dalla scarsa rapidità di risoluzione e, di conseguenza, l'indicazione delle azioni correttive da intraprendere.
- **Monitoraggio delle prestazioni**: le prestazioni dei sistemi vengono monitorate tramite l'analisi di soglie e metriche specifiche per ogni componente, con l'obiettivo di garantire un dimensionamento infrastrutturale in linea con le esigenze di *business* e con valutazioni a livello di costi. L'*outcome* proveniente dal monitoraggio delle prestazioni è di fondamentale importanza per la *road-map* di migrazione dei servizi, in quanto può fornire informazioni a supporto di logiche di *re-platforming* o *re-factoring*.

L'utilizzo di sistemi di *Data Analysis* e *Machine Learning* consente di analizzare le correlazioni presenti fra eventi, livello di disponibilità infrastrutturale e livello di prestazioni. Ad esempio, è possibile rilevare la percentuale di eventi causati da scarse prestazioni dovute ad un dimensionamento non ottimale dei sistemi, oppure si può scoprire che gli eventi a livello di una determinata tipologia di *server* sono stati i più impattanti sul piano della disponibilità rispetto a quelli generati da altre tipologie di *server*.

### 2. Monitoraggio dei sistemi in esercizio

Il monitoraggio, effettuato tramite le funzionalità offerte dall'apposito modulo del sistema di ITSM, ha l'obiettivo di generare azioni correttive puntuali, rispetto ad eventi ad impatto negativo, anticipare azioni migliorative, con l'obiettivo di eludere l'accadimento di eventi negativi e generare una base dati su cui sia possibile produrre *report* a supporto decisionale.
I sistemi oggetto di monitoraggio sono *server*, *storage*, *database* e *network*, offerti alla PA utente.

- Monitoraggio *server*: oltre alla valutazione della disponibilità della macchina, si monitorano: (i) lo stato di *stress* del processore (carico CPU), (ii) lo stato della saturazione della memoria (occupazione RAM) e (iii) i dati relativi alle *performance* in termini di I/O del disco.
- Monitoraggio *database*: si monitorano i parametri significativi a livello delle prestazioni, con l'obiettivo di rilevare margini di ottimizzazione.
- Monitoraggio dei sistemi (SO): si monitorano le metriche e le componenti chiave per il sistema operativo del sistema.

Altre metriche e soglie potranno essere definite, in accordo con il Concedente e con le PA utenti, oltre che le modalità e la frequenza di *reporting*.

### 3. Monitoraggio/reportistica di sicurezza

I servizi di monitoraggio inerenti alla sicurezza si occupano di scannerizzare i sistemi in *real-time*, con l'obiettivo di individuare *change* non opportunamente autorizzate, tracciate o sospette e far emergere potenziali vulnerabilità.
A seconda del tipo di criticità rilevata, si può attivare un sistema di notifica automatico, o l'immediata creazione di un *incident* di sicurezza. Nel secondo caso, il processo di *incident management* viene innescato ed apposita reportistica ne traccia l'evoluzione.

Il servizio di monitoraggio e relativa reportistica di sicurezza include:

- Rilevamento di minacce ed anomalie: supporta l'identificazione di condizioni che potrebbero rivelarsi un obiettivo *target* o un tentativo di *breach* di sicurezza, fornendo evidenza dell'esigenza di azioni di risanamento. Esempi possono includere: informazioni di *login* e *logout*, tentativi andati a buon fine/falliti di inserimento *password*, accessi a *file system* e *database* da parte di utenti specifici.
- Verifica dei controlli di sicurezza: sebbene la maggior parte dei controlli di sicurezza siano orientati a supportare l'applicazione delle indicazioni presenti a livello di *policy*, il monitoraggio viene anche utilizzato per verificare che i controlli stessi operino correttamente; nel caso in cui un evento associabile ad un'azione proibita da una *policy* venisse rilevato e tracciato, questo implicherebbe che il controllo che avrebbe dovuto bloccare quell'azione non è correttamente implementato.
- Identificazione delle vulnerabilità e delle *patch* necessarie: a livello di sistema operativo, eventuali non conformità a *standard* di riferimento sono gestite tramite la prescrizione ed implementazione di *patch*. Dopo aver identificato i sistemi per cui è necessario

applicare delle *patch*, il servizio di monitoraggio fornisce anche evidenza sull'andamento di installazione delle *patch*, tramite dati di distribuzione.

- Generazione di reportistica e di una base dati con valenza legale: per poter consentire alla PA utente di utilizzare i dati provenienti dai sistemi di monitoraggio della sicurezza in un eventuale procedimento legale o penale, l'Offerente propone l'utilizzo di strumenti di conservazione dei dati che ne mantengano integrità verificabile (le registrazioni sono complete e non sono state modificate) per il lasso temporale previsto dalla legge o secondo i requisiti espressi dalla PA stessa.
- Reportistica semestrale in conformità al Dlgs 231/01 e ss.mm.ii.

### 4. Monitoraggio/reportistica di performance dell'infrastruttura

La NewCo renderà disponibile un monitoraggio delle prestazioni, utilizzando il sistema di raccolta delle informazioni statistiche. La raccolta è fatta tramite campionamento quotidiano ad intervalli prefissati (ad esempio ogni 5 minuti) e nelle fasce orarie desiderate. Il tutto viene riportato su una *consolle* grafica di monitoraggio centralizzato che permette una visione aggregata, oltre che l'esportazione delle informazioni verso strumenti di informatica personale quali Microsoft Excel. La raccolta di dati di *performance* può essere personalizzata sia come tipo di contatori (ad esempio, CPU, RAM, disco), sia come famiglie applicative, per valutare lo stato di salute dell'infrastruttura alla base di servizi tecnici e/o di *business* e per poter pianificare eventuali investimenti futuri di ottimizzazione infrastrutturale. In questo secondo caso, è necessario che la PA utente partecipi all'attività fornendo la lista dei raggruppamenti applicativi dei sistemi.
Di seguito, alcuni esempi di *report* relativi alla *performance* infrastrutturale:




*Figura 29: Report di performance dell'infrastruttura*

### 5. Monitoraggio/reportistica applicativo/evolutiva

Relativamente al monitoraggio applicativo/evolutivo, sarà fornita reportistica sui seguenti ambiti:

- Stato di aggiornamento dei sistemi: il *reporting* relativo all'aggiornamento delle *patch* di sicurezza è estratto dal servizio che raccoglie i risultati dello *scan* sulle immagini di sistema operativo e li confronta con il livello di "*patch target*" stabilito in base alla *policy* di riferimento per evidenziare eventuali difformità.
- Stato di obsolescenza dei sistemi: la stessa modalità è implementata per il controllo dell'obsolescenza; in questo caso i dati sono inviati a un portale interno che fornisce *dashboard* regolari sulle componenti *hardware*, *software* e *firmware* che permettono di mantenere sotto controllo le date di "*end of support*" dei prodotti, evitando potenziali fermi dovuti a versioni obsolete.
- Stato di copertura del *licensing*: si prevede la fornitura di un *report* di *Software Licence Management*, ottenuto elaborando i dati dello strumento di *software tracking* ed i dati di *entitlement* delle licenze contenuti negli strumenti di *Asset Management*.
- *Report* dei *software* in uso: il *report* è generato tramite modalità descritta per il punto precedente, ma senza informazioni inerenti alla titolarità.

- **Stato di disponibilità degli applicativi**: sono disponibili due modalità di reportistica rispetto allo stato di disponibilità degli applicativi:
  - vista che aggrega diverse sorgenti dati e mostra lo stato di "*health*" del sistema con una vista per applicazione;
  - vista fornita dal sistema di ITSM che supporta le informazioni di *availability* basate sulla disponibilità delle componenti in funzione degli *incident* rilevati.

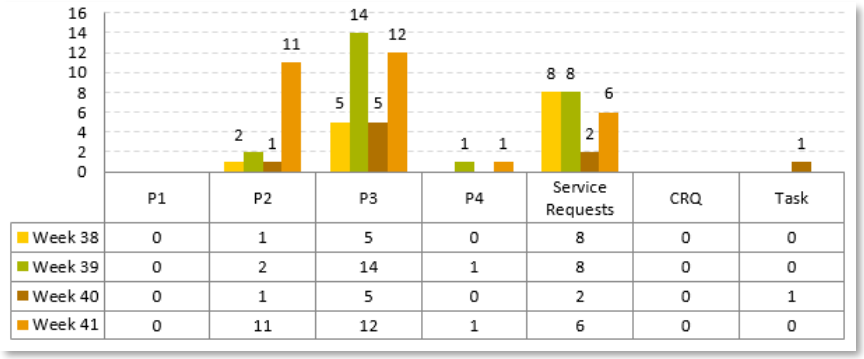
## 6. Reportistica sui ticket

Il rispetto dei livelli di prestazioni accordati (SLA), viene reso evidente tramite il calcolo di appositi KPI. Il *report* riporta le seguenti informazioni: area, KPI, misurazione, valore, fonte, peso e soglia. Di seguito, se ne riporta un esempio:

*Tabella 10: Esempio di report di monitoraggio SLA*

| Area | KPI | Misurazione | Valore | Fonte | Peso | Soglia |
|---|---|---|---|---|---|---|
| Service Management | Puntualità nell'emissione del Service Report | Numero di giorni medio di ritardo nell'emissione del Service Report rispetto al decimo giorno lavorativo del mese successivo a quello di riferimento | 0 | Manuale | 0.50% | <=2gg |
| | Reset Password | Percentuale di ripristino di una password standard per account AD/Notes/VPN entro il tempo soglia di 1 ora | 100.00% | ITSM Tool | 1.00% | >=90% |
| | Modifiche File-share | Percentuale di applicazione delle modifiche sulla struttura di condivisione file entro il tempo soglia di 8 ore | 100.00% | ITSM Tool | 1.00% | >=90% |
| | Creazione Account | Percentuale di creazione di nuovi account sui sistemi in ambito (p.e. AD, Exchange, Sap entro 2 giorni lavorativi dalla richiesta | 100.00% | ITSM Tool | 0.50% | >=90% |
| | Restore | Completamento restore/retrieve dei salvataggi Tivoli entro 1 giorno dalla richiesta | 100.00% | ITSM Tool | 1.00% | >=80% |
| | Servizi DB administrator | Percentuale di evasione richieste entro il tempo soglia di 1 giorno | 100.00% | ITSM Tool | 0.50% | >=90% |
| | Richieste SAP | Percentuale di evasione richieste entro il tempo soglia di 1 giorno | n.c. | ITSM Tool | 0.50% | >=90% |
| Service Desk | Tempo di risposta | Percentuale di chiamate con attesa della risposta di un operatore entro 20 secondi | 95.31% | Contact Centre | 0.50% | >80% |
| | Abbandono delle chiamate | Percentuale di chiamate abbandonate rispetto al totale, nel periodo di osservazione | 0.74% | Contact Centre | 0.50% | <=6% |
| | Disponibilità del servizio di trouble Ticketing | Tempo di disponibilità del servizio rispetto all'orario di servizio | 100.00% | Monitoring Tool | 0.75% | >=95% |
| | Presa in carico incident | Percentuale di incident con priorità alta o emergenza, presi in carico entro 2 ore dalla segnalazione | 100.00% | ITSM Tool | 1.00% | >=95% |
| | Follow up fornitori terzi | Percentuale di ticket nello stato Pending in carico ai fornitori ISAB con almeno un update giornaliero | 100.00% | ITSM Tool | 0.25% | >=95% |
| | Efficacia risoluzione HD1 | Percentuale di ticket risolti da HD1 che non abbiano generato riaperture da parte dei requester | 100.00% | ITSM Tool | 0.50% | >=99% |
| | Tempo di presa in carico in Reperibilità | Percentuale di chiamate assegnate al Servizio di Reperibilità entro 2 ore dalla segnalazione | 100.00% | ITSM Tool | 0.50% | >=99% |
| DataCenter e network management | Disponibilità servizio | Percentuale di disponibilità dei servizi critici (p.e. eMail, BES, CVT, CVM) rispetto all'orario di servizio stabilito | 99.99% | Monitoring Tool | 1.5% | >=99,98% |
| | Disponibilità LAN/WAN | Percentuale di disponibilità degli apparati di rete nell'orario di servizio | 99.98% | Monitoring Tool | 1.50% | >=99,98% |
| | Tempo di reazione Monitoring | Percentuale di incident presi in carico entro 30 minuti dalla segnalazione | 100.00% | Monitoring Tool | 1.50% | >=95% |

Di seguito si riporta un esempio di reportistica relativa ai *ticket*:




| | P1 | P2 | P3 | P4 | Service Requests | CRQ | Task |
|---|---|---|---|---|---|---|---|
| Week 38 | 0 | 1 | 5 | 0 | 8 | 0 | 0 |
| Week 39 | 0 | 2 | 14 | 1 | 8 | 0 | 0 |
| Week 40 | 0 | 1 | 5 | 0 | 2 | 0 | 1 |
| Week 41 | 0 | 11 | 12 | 1 | 6 | 0 | 0 |

*Figura 30: Vista settimanale per diversa tipologia di ticket*

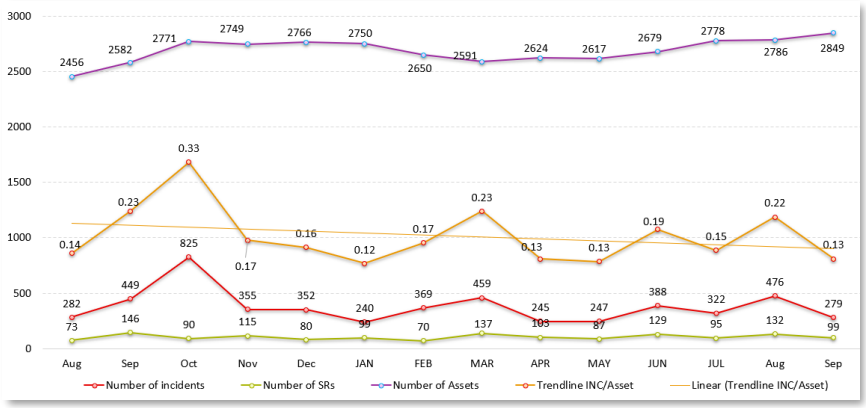



Figura 31: Trend *annuale per diversa tipologia di ticket*

Dal complesso delle migliorie offerte, emerge un concreto ed evidente miglioramento del modello di *governance*, sia societario-amministrativo, che tecnologico-operativo, volto a garantire un maggior coinvolgimento del Concedente, e un più capillare controllo da parte del Concedente, degli Enti preposti e delle PA utenti, anche ai fini di assicurare una maggiore trasparenza ed una maggiore vigilanza e monitoraggio pubblico sull'attività della NewCo come strumento per l'attuazione del PSN.

## 1.18 ID CRITERIO:18 – VALUTATIVO - MIGLIORAMENTI, A FAVORE DEL CONCEDENTE, DELLA *COMPLIANCE* NELL'AGGIORNAMENTO DEI COSTI E PREZZI DELL'INFRASTRUTTURA ANCHE DA UN PUNTO DI VISTA DEL *REFRESH* TECNOLOGICO. TALI MIGLIORAMENTI, PER ESSERE APPREZZATI, DEVONO ESSERE CHIARI, EVIDENTI E, POSSIBILMENTE, MISURABILI.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 18 | Valutazione | Conduzione | Miglioramenti sugli aspetti aggiornamento prezzi | Miglioramenti, a favore del Concedente, della *compliance* nell'aggiornamento dei costi e prezzi dell'infrastruttura anche da un punto di vista del *refresh* tecnologico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili. | **3** |

Con riferimento al criterio 18, si riporta, preliminarmente, quanto disposto dall'art. 5, comma 4 della BdC:

"*Art. 5, comma 4*
*Resta inteso che, sentito il parere del Comitato di Controllo di cui all'art. 12, il contenuto dei Servizi potrà essere, in coerenza con l'art. 175 del Codice, rideterminato consensualmente tra le Parti allo scopo di assicurare:*

*i. l'aggiornamento alle tecnologie, di tempo in tempo rese disponibili sul mercato, purché con cadenza temporale non inferiore a 24 (ventiquattro) mesi rispetto all'aggiornamento precedente, fissando i corrispettivi per i Servizi così modificati con la determinazione di nuovi prezzi, che potranno essere inferiori o superiori a quelli contenuti nei Contratti originari, fermo restando l'equilibrio del PEF ed i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto;*
*ii. l'integrazione dei Servizi con la previsione di nuovi servizi, non originariamente previsti dal Catalogo dei Servizi perché frutto dell'evoluzione tecnologica o gestionale, nonché dell'esperienza maturata nella fornitura dei Servizi, purché con cadenza temporale non inferiore a 24 (ventiquattro) mesi rispetto all'aggiornamento precedente; le Parti procederanno alla determinazione dei nuovi prezzi dei servizi così integrati o aggiornati, fermi restando l'equilibrio del PEF ed i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto;*
*iii. la riduzione del Corrispettivo per i Servizi oggetto dell'Offerta, ai limitati fini dell'adeguamento ai prezzi praticati alle Amministrazioni Utenti secondo il mutare della struttura dei costi del Concessionario, che saranno valutati oggettivamente alla luce delle condizioni di mercato dal Comitato di Controllo di cui all'art. 12, fermi restando sia l'equilibrio del PEF che i limiti previsti dalla legislazione vigente per la variazione delle prestazioni in costanza di contratto; resta altresì inteso e condiviso tra le Parti che tale revisione non potrà comunque intervenire prima del terzo anno dalla sottoscrizione della presente Convenzione e successivamente con cadenza biennale."*

Al fine di porre in essere un efficace e sostenibile processo di aggiornamento dei costi di gestione e di aggiornamento tecnologico dell'infrastruttura che porti benefici in termini di minori costi alle Amministrazioni, di efficientamento delle infrastrutture e dei servizi del PSN, nonché di evoluzione continua e migliorativa dei servizi erogati, nel confermare l'aderenza a quanto previsto nella documentazione di gara (in particolare, art. 5, comma 4 della BdC), si offre, come miglioria tangibile rispetto agli aspetti disciplinati dal suddetto articolo della BdC, un sistema di gestione avanzato, in grado di rendere più efficiente, più trasparente e più conveniente tale processo per il Concedente e per le Amministrazioni utenti.
In particolare, il sistema oggetto di offerta è volto a garantire una metodologia affidabile e trasparente per:

- affrontare la revisione dei prezzi obbligatoria, di cui all'art. 5, comma 4, punto iii della BdC, garantendo un risparmio stabile e programmato per le PA utenti e, al contempo,
- gestire nella maniera più efficiente l'analisi dei costi relativi alle eventuali modifiche contrattuali previste dall'art. 5, comma 4, punti i. ed ii. della BdC,
- assicurando un'affidabile metodologia per l'individuazione e la gestione del *refresh* tecnologico.

Il sistema proposto nella presente Offerta sarà, pertanto, articolato in 4 fasi, di seguito dettagliatamente descritte:

1. **ottimizzazione** dei servizi e dei relativi costi e prezzi, grazie ad un approccio innovativo che ricorre a strumenti di ***Artificial Intelligence*** (cfr. *infra* par. 1.18.1);
2. procedura di individuazione del ***benchmark*** **dei prezzi** che garantisce la piena aderenza ai *trend* di mercato di servizi analoghi (cfr. *infra* par. 1.18.2);
3. uno **sconto prefissato** da applicare ai prezzi rideterminati nella precedente fase di revisione, che garantisce condizioni migliorative e misurabili a priori (cfr. *infra* par. 1.18.3);
4. un **processo di *refresh* tecnologico**, svolto grazie ad un'attenta analisi delle innovazioni presenti sul mercato, condotta attraverso consultazioni di più attori come elemento

qualitativo dell'infrastruttura e dei servizi e come ulteriore elemento per l'ottimizzazione dei costi e, quindi, per la riduzione del corrispettivo dei servizi (cfr. *infra* par. 1.18.4).

### 1.18.1 Ottimizzazione di servizi e costi attraverso l'utilizzo di strumenti di AI

Si offre un'attività di monitoraggio, rilevazione ed acquisizione di parametri tecnici e di dati amministrativo/contabili relativi ai servizi oggetto della concessione. Tali dati verranno elaborati attraverso specifici strumenti di AI su un'ampia mole di dati (cd "*Big Data*") attraverso specifiche funzionalità di *Analytics*. Grazie all'elaborazione in parola, sarà possibile individuare (dal punto di vista tecnico e contrattuale) le migliori aggregazioni di servizi oggetto della concessione, così da definire il perimetro di macro-servizi o di applicazioni articolate da offrire alle Amministrazioni utenti.
Tale attività garantisce l'aderenza continua ai fabbisogni evolutivi ed agli usi effettivi dei servizi da parte delle Amministrazioni dell'infrastruttura PSN, permettendo un innalzamento del livello qualitativo dei servizi offerti, e fornisce alle PA utenti una chiara indicazione per la migliore scelta dei servizi dal punto di vista del dimensionamento, del *mix* tecnologico e dei costi.

Ne deriva anche un utilizzo ottimizzato di tutta l'infrastruttura del PSN, con conseguente riduzione dei sovradimensionamenti della stessa o della frammentazione delle risorse, con relativo impatto sui costi dell'infrastruttura.

Dunque, le funzionalità di AI valorizzano il patrimonio dei dati operativi e contrattuali generati massivamente, trasformandolo in informazioni utili per le analisi dei fabbisogni attraverso i seguenti *output*:

- Individuazione delle *best practice* in esercizio;
- Definizione dei *bundle* di servizi ottimizzati, al fine di ampliare il catalogo con macro-servizi volti all'erogazione di servizi/applicazioni complesse;
- Correlazione ottimale tra differenti servizi che vengono sottoscritti dalle Amministrazioni, al fine di arricchire *bundle* di servizi elementari con le opzioni innovative frequentemente richieste dalle Amministrazioni ed estendere il catalogo con nuovi servizi/applicazioni evoluti ed ottimizzati in termini di risorse, costi e tempi di implementazione;
- Scelta del *mix* ottimale di tecnologie per l'erogazione dei servizi;
- Calcolo del tasso di utilizzo nel tempo dei servizi, in termini di risorse impegnate e sottoscrizioni contrattuali, al fine di ottimizzare i servizi del catalogo e le risorse impegnate e, conseguentemente, i costi dell'infrastruttura.

### 1.18.2 Procedura di individuazione del *benchmark* dei prezzi ai fini della revisione

A norma dell'art. 12 della BdC, il Comitato ha, tra gli altri, il compito di

- verificare l'andamento dei prezzi dei servizi del PSN e gli altri termini ai quali questi sono resi alle Amministrazioni, *"in relazione ai prezzi ed alle tecnologie comparabili presenti sul mercato, avendo sempre riguardo all'incidenza sull'equilibrio del piano economico finanziario*", nonché, per quanto qui di interesse, di
- "*supportare il Concedente ed il Concessionario attraverso: […] l'espressione del parere consultivo di cui all'art. 5, comma 4 e l'effettuazione delle valutazioni di cui al punto iii. di quest'ultimo comma*".

Nell'ambito dello svolgimento dei predetti compiti, il sistema oggetto della presente Offerta propone l'approccio metodologico descritto di seguito:

- il Comitato effettuerà un'approfondita indagine di *benchmark* atta a rilevare i migliori prezzi di mercato di servizi analoghi a quelli erogati con il PSN in contesti equiparabili per criticità, dimensioni, tecnologie, Livelli di Servizio ed estensione territoriale, debitamente compensati alle realtà, alle infrastrutture ed ai criteri del PSN;
- a tal fine, il Comitato potrà conferire, con decisione congiunta dei propri membri, mandato a un "*accreditato operatore di mercato*" con comprovata esperienza;
- l'obbiettivo di questa attività sarà quella di definire il termine di confronto sull'andamento dei prezzi medi di mercato dei servizi offerti dal PSN. A tal fine, l'analisi di mercato potrà:
    - individuare i maggiori operatori nazionali ed internazionali operanti sul mercato italiano che eroghino servizi analoghi;
    - individuare un campione di confronto (*peer*) di almeno cinque offerte ciascuna delle quali dovrà avere a listino almeno il 70% dei servizi offerti dal PSN; ogni servizio deve essere presente in almeno tre delle cinque offerte;
    - allineare e ricondurre le metriche dei servizi individuati nei diversi peer a quelli del PSN;
    - introdurre eventuali elementi correttivi dei prezzi, qualora i servizi individuati si discostino, in maniera misurabile, da quelli erogati dal PSN;
    - calcolare il prezzo di riferimento di mercato per ciascuna classe di servizio, come media dei tre migliori prezzi del *benchmark*;
    - verificare i prezzi medi del *benchmark* e confrontarli con i prezzi iniziali contrattuali, per classe di servizio.

Tale metodologia potrà essere utilizzata sia ai fini della revisione dei prezzi, a norma dell'art. 5, comma 4, punto iii della BdC, sia come riferimento per i nuovi prezzi da individuare nel caso di aggiornamento delle tecnologie, o introduzione di nuovi servizi, conformemente a quanto previsto dall'art. 5, comma 4, punti i. e ii. della BdC.

### 1.18.3 Sconto migliorativo prefissato e garantito

Lo strumento di AI di cui alla presente Offerta e la conseguente ottimizzazione dei servizi e dei costi dell'infrastruttura, sopra descritte, consente di offrire, fin da ora, **una condizione migliorativa per la revisione dei prezzi, rispetto a quanto previsto dall'art. 5, comma 4, lett. iii della BdC**.

In merito, si offre un **valore di sconto minimo prefissato, pari, almeno, al 2% (due per cento) dopo il primo biennio – dunque, in maniera anticipata rispetto a quanto previsto nell'art. 5, comma 4, punto iii. della BdC - e all'1% (uno per cento) per i restanti bienni di durata della Convenzione**.
Tale sconto sarà applicato ai prezzi ridefiniti nella fase di *benchmark*, di cui al precedente paragrafo 2, qualora, in esito al suddetto processo, lo scostamento tra i prezzi rilevati ed i prezzi di listino dovesse risultare inferiore al 2% dopo il primo biennio o al 1% nei successivi bienni.

Ne deriva che, nel caso in cui il processo di *benchmark* restituisca un prezzo più basso in misura:
- **inferiore** al 2% (per il primo biennio) o al 1% (per i restanti bienni), verrà comunque riconosciuto uno sconto pari, rispettivamente, al 2% (due per cento) o all'1% (uno per cento);
- **superiore** al 2% (per il primo biennio) o al 1% (per i restanti bienni), verrà riconosciuto lo sconto pari a quello derivante dal processo di *benchmark*.

Tale approccio assicurerà una diretta misurabilità e trasparenza del criterio migliorativo offerto e dei conseguenti vantaggi fruibili dal Concedente e dalle Amministrazioni, attraverso l'innovativo meccanismo di AI predisposto dal Concessionario.

### 1.18.4 Aggiornamento Tecnologico

L'Offerta prevede, inoltre, che, parallelamente e con la stessa periodicità prevista per la revisione dei prezzi, di cui al precedente paragrafo 1.18.3, il Concessionario svolga un'analisi delle innovazioni tecnologiche, ai fini dell'applicazione di quanto previsto dall'art. 5, comma 4, punti i. e ii. della BdC, mediante il supporto dello strumento di AI sopra descritto e consultazioni di mercato che coinvolgano i maggiori fornitori di tecnologie e le principali Amministrazioni, volte ad introdurre nuovi servizi e/o aggiornamenti dell'infrastruttura che impattano in termini di (i) fruibilità dei servizi; (ii) aumento della sicurezza; (iii) efficienza dell'infrastrutture e delle risorse; (iv) efficientamento energetico delle infrastrutture utilizzate dal PSN.

Tale processo sarà finalizzato a:

- proporre nell'ambito del Comitato gli aggiornamenti tecnologici individuati e valutati positivamente in relazione all'impatto sull'erogazione dei servizi;
- fissare la *roadmap* di implementazione di tali aggiornamenti e nuovi servizi;
- individuare i prezzi dei nuovi servizi introdotti con il conseguente aggiornamento del listino;
- valutare le eventuali variazioni di prezzo conseguenti all'aggiornamento (aumento, conferma o diminuzione);
- verificare la sussistenza delle condizioni normative per introdurre tali modifiche, in funzione della compatibilità con le condizioni contrattuali e con le disposizioni in materia, con particolare riferimento all'art. 175 del Codice.

## 1.19 ID CRITERIO:19 – VALUTATIVO - MIGLIORAMENTI SULLA PROPOSTA PROGETTUALE PER QUANTO RIGUARDA GLI ASPETTI RELATIVI ALL'INTEGRAZIONE DEL PSN CON L'ARCHITETTURA NAZIONALE CYBER, CON PARTICOLARE RIGUARDO ALLE MODALITÀ ED AI PROCESSI PER L'INTEGRAZIONE CON LO CSIRT ITALIA (FINO A 1 PUNTO), ALLA MESSA A DISPOSIZIONE DI FUNZIONALITÀ PER L'INTERAZIONE CON GLI ISAC (FINO A 1,5 PUNTI), MESSA A DISPOSIZIONE DI FUNZIONALITÀ PER SCAMBIO DI INFORMAZIONI A2A TRA IL SOC E LO CSIRT ITALIA (FINO A 2,5 PUNTI)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 19 | Valutazione | Cybersecurity | Miglioramento degli aspetti cybersicurezza dell'infrastruttura. | Miglioramenti sulla proposta progettuale per quanto riguarda gli aspetti relativi all'integrazione del PSN con l'Architettura Nazionale *Cyber*, con particolare riguardo alle modalità ed ai processi per l'integrazione con lo CSIRT Italia (fino a 1 punto), alla messa a disposizione di funzionalità per l'interazione con gli ISAC (fino a 1,5 punti), messa a disposizione di funzionalità per scambio di informazioni A2A tra il SOC e lo CSIRT Italia (fino a 2,5 punti). | **5** |

### 1.19.1 Introduzione

Come sottolineato dal MITD, nel suo complesso, la digitalizzazione aumenta il livello di esposizione della società rispetto a minacce *cyber* su tutti i fronti. Per far fronte a questa problematica, il Piano per l'Italia digitale 2026 contiene importanti misure di rafforzamento delle nostre difese *cyber*, a partire dalla piena attuazione della disciplina in materia di "*Perimetro di Sicurezza Nazionale Cibernetica*" ("PSNC"). In primo luogo, viene rafforzata la sicurezza dei sistemi informativi italiani contro i rischi derivanti dalla criminalità informatica, agendo sui presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettati verso la Pubblica Amministrazione e le imprese di interesse nazionale. In secondo luogo, viene rafforzata la capacità di condivisione delle informazioni tra diversi soggetti in merito agli eventi di sicurezza occorsi o che potrebbero verificarsi, attraverso il rafforzamento o l'istituzione *ex novo* di strutture atte a raccogliere ed analizzare gli eventi, gli incidenti, le nuove minacce e le vulnerabilità. In terzo luogo, sono costruite o rese più solide le capacità tecniche di valutazione ed a*udit* continuo della sicurezza di apparati elettronici ed applicazioni utilizzati per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale: ciò ha portato all'istituzione del Centro di Valutazione e di Certificazione Nazionale ("CVCN"), istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia per la cybersicurezza nazionale, e degli altri Centri di Valutazione ("CV") per la valutazione di prodotti in acquisizione da parte dei soggetti inclusi nel PSNC.
In tale scenario, le infrastrutture, le modalità di condivisione delle informazioni ed i processi che la NewCo propone rappresentano un elemento chiave del contesto dell'architettura nazionale *cyber* e ne sposano principi ed obiettivi, come esplicitato nei seguenti paragrafi.

### 1.19.2 Infrastruttura per il PSNC

### 1.19.3 Le infrastrutture PSNC e gli obiettivi comuni con il PNRR

La NewCo si doterà di idonee unità organizzative al fine di garantire ed assicurare la tutela delle infrastrutture e dei servizi considerati essenziali agli interessi nazionali ed alla sicurezza nazionale. Queste infrastrutture saranno sia all'interno della NewCo stessa che supportate dalle infrastrutture dell'Offerente. In particolare, la NewCo si doterà di *Security Operation Center* (SOC) e di *Computer Emergency Response Team* (CERT) e garantirà tutti i livelli di sicurezza previsti dalle normative vigenti al fine di mantenere la presenza di un ambiente sicuro e protetto. In questo contesto, è importante sottolineare il ruolo svolto da Fastweb all'interno della NewCo, grazie alla visibilità su eventi di sicurezza derivante non solo dal monitoraggio dei dati delle PA utenti, ma anche sulla base delle informazioni raccolte dal SOC, dal CERT e dallo CSIRT di Fastweb nelle quotidiane attività di monitoraggio. In particolare, la costante attività di monitoraggio degli eventi di sicurezza da parte del SOC di Fastweb contribuisce in maniera rilevante alla stesura del "*Rapporto CLUSIT sulla sicurezza ICT in Italia*". In questo contesto, si registra un forte aumento degli eventi malevoli nel 2021, che sono stati circa 42 milioni con un incremento del +17% rispetto all'anno precedente.
Tutte le iniziative della NewCo prenderanno in considerazione le indicazioni derivanti dal Piano Nazionale di Ripresa e Resilienza (PNRR), con particolare *focus* sugli aspetti più collegati alla misura *M1C1 - 1.5: Cybersecurity* per la quale sono previsti 623 milioni di Euro di investimento. Tale misura, resa attuativa attraverso il DL 82/2021 che istituisce l'Agenzia per la cybersicurezza nazionale (ACN), si pone l'obiettivo di rafforzare la sicurezza dei sistemi informativi italiani contro i rischi derivanti dalla criminalità informatica, garantendo la piena attuazione della disciplina in materia di Perimetro di Sicurezza Nazionale Cibernetica (PSNC), in linea con i requisiti di sicurezza della direttiva (UE) 2016/1148. In quest'ottica, la NewCo attuerà una serie di iniziative volte a garantire la protezione proattiva delle PA utenti ed a svolgere il ruolo di ISAC (*Information Sharing and Analysis Center*) per la condivisione delle informazioni rilevanti dal punto di vista della *cybersecurity* su scala nazionale ed europea.

### 1.19.4 Recepimento di normative nazionali ed europee e conformità a standard di sicurezza

La NewCo, oltre a perseguire gli obiettivi definiti nel PNRR, avrà l'obiettivo di:

- assicurare la conformità alle leggi ed ai regolamenti applicabili, tra cui quelle relative alla sicurezza delle informazioni, alla tutela dei dati personali nonché quelle applicabili agli Operatori dei Servizi Essenziali (OSE), ai Fornitori di Servizi Digitali (FSD) ed ai soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC);
- garantire una protezione dell'informazione adeguata in termini di confidenzialità, integrità e disponibilità;
- proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- assicurare misure tecniche ed organizzative per la protezione dell'informazione e la gestione dei rischi correlati, descritte da specifiche *policy* di sicurezza e soggette a certificazione ISO/IEC 27001 ed ISO 22301 nonché in conformità a tutte le normative applicabili ed elencate di seguito.

Le principali esigenze di sicurezza, tenendo in considerazione l'evoluzione costante del contesto normativo e tecnologico fortemente enfatizzato dalla pubblicazione recente di direttive, regolamenti, decreti e norme sia a livello UE che nazionale, riguardano:

- la presenza di un ambiente sicuro e protetto;
- la protezione dei dati personali trattati;
- la conformità normativa e di settore del Centro Servizi e dei clienti.

La progettazione dei servizi erogati dalla NewCo prenderà in considerazione il contesto normativo in cui il PSN e le PA utenti si troveranno ad operare. In particolare, saranno prese in considerazione tutte le normative vigenti che, direttamente o indirettamente, impattano sui servizi erogati dal PSN. I requisiti di sicurezza derivanti dalle normative saranno implementati tenendo a riferimento gli *standard* e le *best practice* di settore per la realizzazione e gestione dei servizi informatici nel rispetto dei principi di sicurezza.
I principali riferimenti considerati in fase di sviluppo dei servizi e per la loro futura erogazione includono i seguenti elementi:

- **Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali,** definita nel DPCM del 17/02/2017;
- **Recepimento della direttiva NIS (UE 2016/1148) per la definizione delle misure di sicurezza necessarie per la protezione degli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali,** definito nel D. Lgs. 65/2018;
- **Perimetro di Sicurezza Nazionale Cibernetica,** definito nel D.L. 105/2019 e ss.mm.ii. (L. 18 novembre 2019, n. 133 e D.L. 82/2021);
- Disposizioni urgenti in materia di *cybersicurezza*, definizione dell'architettura nazionale di *cybersicurezza* ed istituzione dell'Agenzia per la cybersicurezza nazionale, definito nel **D.L. 82/2021**;
- **Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici**, definito nel DPCM n. 81 del 14 aprile 2021;
- Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, definito nel **DPCM 15 giugno 2021**;
- **Regolamento UE 2016/679 del Parlamento europeo e del Consiglio** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla

Protezione dei Dati o GDPR) e relativi adeguamenti descritti nel D.Lgs. 196/2003 e ss.mm.ii. con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101;

- Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un **livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione**, definito nel D.L. 65/2018;
- **Piano triennale per l'informatica nella Pubblica Amministrazione** sviluppato da AgID;
- **Codice dell'Amministrazione Digitale,** definito nell'ambito del D.Lgs. 7 marzo 2005 e ss.mm.ii.;
- Disposizioni sull'organizzazione ed il funzionamento del *Computer security Incident Response Team* - CSIRT italiano, definite nel **DPCM 8 agosto 2019**;
- Regolamento in materia di perimetro di sicurezza nazionale cibernetica (Obblighi censimento beni ICT, Analisi del Rischio), definito nel **DPCM 30 luglio 2020, n. 131**;
- Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, **definito nel DPR 5 febbraio 2021, n. 54** (Procedure e termini per le valutazioni da parte del CVCN sui servizi e le forniture).

Gli *standard*, le linee guida e le *best practice* che saranno presi in considerazione per la realizzazione e la gestione dei servizi comprendono:

- **Piano nazionale per la protezione cibernetica e la sicurezza informatica**;
- ***Framework nazionale di cyber security e data protection***;
- NIST *Cyber Security Framework*;
- **Criteri per la qualificazione dei *Cloud Service Provider* per la PA,** CIRCOLARE N. 2 del 9 aprile 2018 di AgID;
- **Misure minime di sicurezza informatica per la PA definite da AgID**;
- **Famiglia dello standard ISO/IEC 27000** (Adozione, Implementazione e gestione di un Sistema di Gestione per la Sicurezza delle Informazioni) ed in particolare:
  - **ISO/IEC 27001** – *Information technology — Security techniques — Information security management systems — Requirements*;
  - **ISO/IEC 27002** – *Information technology — Security techniques — Code of practice for information security controls*;
  - **ISO/IEC 27701** – *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*;
  - **ISO/IEC 27017** – *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;*
  - **ISO/IEC 27018 –** *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*;
  - **ISO/IEC 27005** – *Information technology — Security techniques — Information Security risk management*;
  - **ISO/IEC 27035-1** *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*;
  - **ISO/IEC 27035-2** *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response;*

  - ISO/IEC 27035-3 *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations;*
- ISO 9001 (Adozione, Implementazione e gestione di un Sistema di Gestione per la Qualità dei processi);
- ISO 9004 *Quality of an organization -- Guidance to achieve sustained success*;
- ISO 20000-1 (Adozione, Implementazione e gestione di un Sistema di Gestione per l'ICT *Service Management*);
- ISO 20000-2 *Guidance on the application of service management systems*;
- ISO 22301 (Adozione, Implementazione e gestione di un Sistema di Gestione della Continuità Operativa);
- ISO 31000 - Gestione del rischio - Linee guida;
- *Cloud Security Alliance Controls*.




*Figura 32: Ruolo strategico della Cybersecurity - Fonte: AgiD Italia digitale 2026*

### 1.19.5 Supporto alle iniziative del PNRR

La tabella seguente riporta le aree di investimento identificate nel PNRR nell'ambito della misura M1C1 – 1.5 *Cybersecurity* che saranno supportate, direttamente o indirettamente, dalle iniziative introdotte dalla NewCo.

*Tabella 11: Aree PNRR supportate dalle iniziative della NewCo*

| Ambito | Iniziativa | Deadline | Proposta della NewCo |
|---|---|---|---|
| Creazione dell'infrastruttura per il PSNC | Implementazione di una struttura operativa *core*: un ISAC nazionale (centrale) in connessione con il *Cyber Shield* dell'UE e un insieme di *hub* dedicati (virtuali) di "risposta alle emergenze" ("CERTS settoriali/regionali", incentrati su settori industriali definiti in modo coerente con il PSNC e la NIS, e/o aree territoriali). | 2024 | La NewCo si strutturerà come ISAC per la condivisione delle informazioni con potenziale impatto sulla *cybersicurezza* nazionale (cfr. "Interazione con l'ISAC e CSIRT Italia") includendo anche le informazioni raccolte da Fastweb attraverso il monitoraggio di eventi di sicurezza relativi ai suoi clienti. |
| Creazione dell'infrastruttura per il PSNC | Realizzazione di Strumenti tecnologici: *high-performance computing* (HPC) e un sistema di modellazione e tracciamento dedicato per gli *asset* ICT strategici inclusi nel PSNC. | 2023 | La NewCo si rende disponibile a integrare ed ospitare sistemi di HPC all'interno dei suoi DC per supportarne l'adozione (cfr. "*High Performance Computing* e Simulazione tramite intelligenza artificiale e *Machine Learning*") al fine di integrare le capacità computazionali con l'ampia base informativa a disposizione di Fastweb e del PSN. |

| Ambito | Iniziativa | Deadline | Proposta della NewCo |
|---|---|---|---|
| Creazione dell'infrastruttura per il PSNC | Istituzione dell'Agenzia Nazionale per la *cybersicurezza*, che incorporerà il futuro centro di coordinamento nazionale, da istituire a seguito del regolamento (di prossima adozione) su *European Cybersecurity Competence Network and Centre*. Questa nuova entità avrà il compito di sostenere lo sviluppo delle imprese di *cybersecurity* in Italia, compreso lo *scale-up* delle PMI e delle *start-up* esistenti. | 2022 (attuata nel DL 82/2021) | La NewCo rappresenterà un elemento chiave per le attività di formazione in ambito *cybersecurity*, avvalendosi delle competenze già maturate da Fastweb in questo campo grazie alla Fastweb *Digital Academy* (cfr. "Fastweb *Digital Academy*").<br>Inoltre, saranno valutate nuove opportunità di formazione per le imprese e per i cittadini. |
| Creazione dell'infrastruttura per il PSNC | "*Tech screening*" *network*: laboratori di *screening* tecnologico dedicati, guidati dal CVCN (*National cybersecurity screening and certification laboratory*), per testare e valutare apparecchiature/*asset hardware* e *software* su tutto il territorio nazionale, coerentemente con il quadro europeo di certificazione della *cybersecurity*. | 2024 | La NewCo attraverso i servizi erogati dal CERT in ambito "*Product Evaluation and Certification*" potrà fornire un contributo alla selezione ed alla valutazione di sicurezza di prodotti *hardware* e *software* di interesse per il territorio nazionale. |
| Rafforzamento delle strutture operative | «*National hyper* SOC» (centrale) per il monitoraggio e l'elaborazione di eventi sospetti che hanno luogo all'interno del perimetro nazionale di sicurezza informatica. | 2023 | La NewCo, direttamente o attraverso Fastweb, potrà attestarsi come uno dei 5 centri operativi di sicurezza nazionale da integrare con quello centrale, avvalendosi del *framework* architetturale di Fastweb e composto da tecnologie, processi e risorse professionali specializzate (cfr. "*National Hyper*SOC"). |
| Rafforzamento delle strutture operative | Realizzazione di strumenti/ambienti di simulazione AI/ML finalizzati a comprendere meglio le tattiche e le procedure (TTP) dei moderni attacchi informatici gravi/su larga scala per migliorare la previsione degli scenari post-incidente e la valutazione del rischio sistemico (valutando anche gli effetti a cascata relativi alle interdipendenze tra le infrastrutture critiche), principalmente entro il 2023. | 2023 | Avvalendosi delle capacità di *High Performance Computing* (cfr. "*High Performance Computing* e Simulazione tramite intelligenza artificiale e *Machine Learning*") la NewCo potrà eseguire analisi di dati volte ad esaminare i dati di traffico e correlare eventi di sicurezza al fine di identificare nuove minacce e modalità di attacco. |
| Rafforzamento delle strutture operative | *Software screening* e unità di certificazioni. | 2023 | La NewCo, attraverso i servizi erogati dal CERT in ambito "*Product Evaluation and Certification*" e grazie al supporto dato ai CVCN e CV nazionali, potrà fornire un contributo alla selezione ed alla valutazione di sicurezza di prodotti *hardware* e *software* di interesse per il territorio nazionale (cfr. "*Tech Screening Network*"). |
| Rafforzamento delle strutture operative | Supporto/incentivo alle PA ed alle imprese incluse nel PSNC e nel NIS, finalizzato all'introduzione di nuove capacità di *cybersecurity* nelle PA ed al sostegno del rafforzamento delle misure di *cybersecurity* nelle imprese. | 2024 | La NewCo si pone l'obiettivo di supportare le PA utenti nell'evoluzione delle proprie capacità di protezione attraverso attività di formazione mirata (cfr. "Fastweb *Digital Academy*" e "Supporto a PA"). |

### 1.19.6 Interazione con l'ISAC e CSIRT Italia

Con l'obiettivo di creare l'infrastruttura per il PSNC (coerentemente con la NIS ed altre iniziative europee), attraverso una struttura operativa *core*, ovvero un ISAC nazionale (centrale) in connessione con il *Cyber Shield* dell'UE e un insieme di *hub* dedicati (virtuali) di "*risposta alle emergenze*" ("CERTS settoriali/regionali", incentrati su settori industriali definiti), entro il 2024, la

NewCo si propone di rappresentare uno dei promotori/sponsor principali dell'attività e di mettere a disposizione numerose funzionalità per l'interazione con gli ISAC. In particolare, si propone sia come ISAC di settore che come entità a disposizione per progetti pilota o come "*early adopter*". Il tema della condivisione delle informazioni nell'ISAC viene affrontato dalla NewCo in modo diffuso, anche con una particolare attenzione verso tematiche e possibili interazioni emergenti o emergenziali come il contesto dell'*information warfare*. La NewCo si propone anche di dotarsi delle infrastrutture tecnologiche necessarie a raggiungere questi obiettivi.

In questo contesto e sulla base di questi obiettivi, risulta indispensabile comprendere come la condivisione delle analisi sia una delle principali sfide nella costruzione dell'ecosistema ISAC in Europa.
Far parte di un ISAC richiede di dedicare risorse, tempo e competenze; nel settore privato questo può essere costoso, quindi la motivazione deve essere forte. La condivisione delle conoscenze sulla sicurezza informatica e delle informazioni sulla risposta agli incidenti sono tra i motivi più comuni per partecipare a un ISAC.
I membri degli ISAC si scambiano informazioni su minacce, incidenti, vulnerabilità, misure di mitigazione ed anche su *tool* e *best practice*. In tale contesto la NewCo propone lo scambio di informazioni relativo ai seguenti punti:

- incidenti: dettagli di attacchi tentati e riusciti che possono includere una descrizione delle informazioni oggetto di perdite di riservatezza, integrità o disponibilità, le tecniche utilizzate, l'intento e l'impatto. La gravità di un incidente potrebbe variare da un attacco bloccato con successo a una grave situazione di sicurezza nazionale;
- minacce: problematiche, ancora da comprendere, con implicazioni potenzialmente gravi; informazioni sugli attori delle minacce; indicatori di compromissione (IoC), come *file* dannosi, indirizzi *e-mail* rubati, indirizzi IP interessati o campioni di *malware*. Le informazioni sulle minacce possono aiutare gli operatori a rilevare o scoraggiare gli incidenti, imparare dagli attacchi e creare soluzioni in grado di proteggere meglio i propri sistemi e quelli di terzi;
- vulnerabilità: problematiche *software*, *hardware* o nei processi aziendali che possono essere sfruttati per scopi dannosi;
- mitigazioni: metodi per rimediare alle vulnerabilità, contenere o bloccare le minacce e rispondere agli incidenti e ripristinare l'operatività. Le forme comuni di tali informazioni includono *patch* per bloccare le vulnerabilità, aggiornamenti antivirus per fermarne lo sfruttamento ed indicazioni per eliminare gli attori malintenzionati dalle reti;
- consapevolezza della situazione (*situational awareness*): informazioni che consentono ai responsabili delle decisioni di rispondere a un incidente e che potrebbero richiedere la telemetria in tempo reale delle vulnerabilità sfruttate, delle minacce attive e degli attacchi. Tali informazioni potrebbero anche contenere elementi di interesse in merito agli obiettivi degli attacchi e allo stato delle reti d'importanza critica pubbliche o private;
- *best practice*: informazioni relative al modo in cui il *software* ed i servizi vengono sviluppati e forniti, come controlli di sicurezza, pratiche di sviluppo sicuro e risposta agli incidenti e parametri di efficacia o *patching* del *software*;
- analisi strategica: raccolta ed analisi di molti tipi di informazioni per creare metriche, tendenze e proiezioni. A supporto di tale analisi si utilizzano proiezioni di potenziali scenari per preparare i responsabili delle decisioni del governo o del settore privato a rischi futuri.

In ottica di azioni di mitigazione del rischio diventa quindi fondamentale lo scambio di informazioni riguardante questi punti, così come descritto nella seguente immagine:

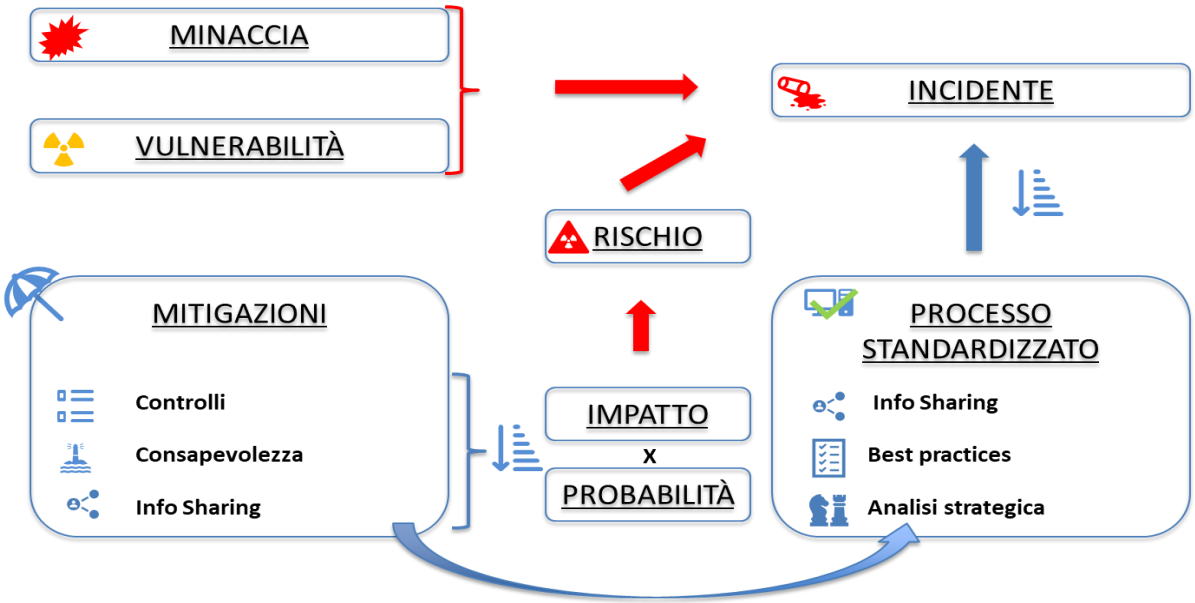



*Figura 33: Scambio informazioni per la mitigazione del rischio*

La NewCo si propone come ISAC di settore con la capacità di collezionare e condividere informazioni derivanti da diverse sorgenti. Questo tipo di cooperazione si concentra sul settore di cui fa parte il PSN nell'ambito delle infrastrutture critiche o servizi essenziali/vitali. L'obiettivo è condividere informazioni ed analisi con altri esperti di sicurezza attivi nel settore, in modo che l'operatore possa beneficiare il più possibile delle conoscenze e dell'esperienza rilevanti. Infatti, gli ISAC diventano sovente una piattaforma per servizi condivisi. Le caratteristiche tipiche afferenti ad un ISAC di settore sono quelle descritte nell'immagine seguente (fonte ENISA):

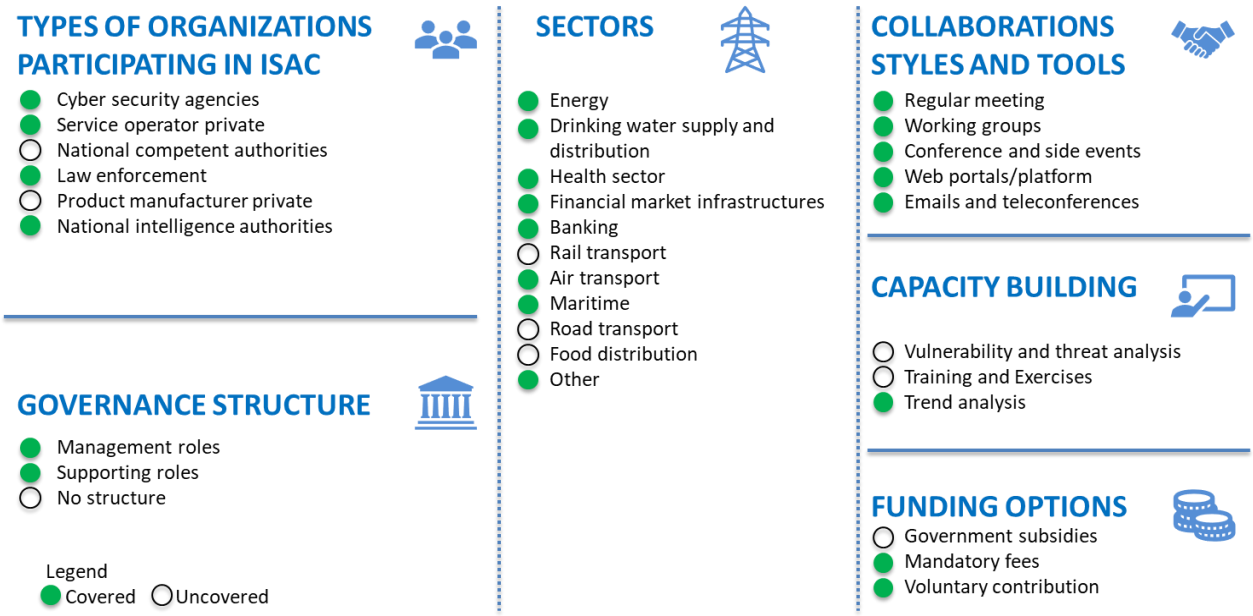



*Figura 34: Caratteristiche ISAC*

Nello specifico la NewCo si pone l'obiettivo di integrare tutti gli strumenti di *information sharing* in ottica di dialogo con il CSIRT Italia, mettendo a disposizione anche funzionalità per lo scambio delle informazioni. In particolare, ci sarà una doppia infrastruttura con un dialogo

costante tra il CERT di Fastweb e lo CSIRT Italia che faciliterà la segnalazione di incidenti ed eventi rilevanti sulla base delle categorie definite nel DPCM 81/2021, avendo Fastweb già da tempo convenzioni con le istituzioni in questo ambito: dal 2013 con il CERT del MISE e dal 2019 con il CNAIPIC. Inoltre, Fastweb è *Trusted Introducer* nella rete dei CERT europei attraverso una delle società del gruppo che opera specificatamente nel campo della *cybsersecurity* e che potrà essere coinvolta nell'ambito della NewCo.

Oltre allo scambio di informazioni vi è la possibilità di svolgere attività nell'ambito dell'obiettivo fissato dall'ISAC. Tali attività comportano un impegno esteso tra i membri e nello specifico quelle che la NewCo andrà ad implementare a tendere sono le seguenti:

- pubblicazione di *white paper* tematici;
- analisi del panorama delle minacce;
- organizzazione di *workshop*, formazione ed esercitazioni;
- presentazione dell'ISAC, delle sue competenze e risultati in conferenze di settore;
- realizzazione di visite educative;
- conduzione di revisioni per le organizzazioni membri, per fornire indicazioni sulle misure di sicurezza.

I parametri operativi, le prestazioni e l'impatto dell'ISAC saranno costantemente sottoposti a misurazioni ed analisi, nel contesto dei processi di miglioramento continuo.

È fondamentale che gli ISAC tengano presente il progressivo processo di scambio di informazioni. Minacce, frodi ed incidenti cambiano natura, costringendo i membri a valutare la necessità di nuovi servizi e misure di mitigazione. Allo stesso modo, la legislazione, le reti e le organizzazioni si sviluppano e cambiano, il che potrebbe costringere gli ISAC ad adattarsi a nuovi contesti. Pertanto, oltre ai processi di valutazione del contesto interno, sono fondamentali anche quelli del contesto esterno: tali valutazioni saranno messe in atto sia in maniera costante e periodica, che sulla base di qualsiasi nuova necessità emergente.
La proposta dell'Offerente, in questo senso, è quella di fornire dei dati misurabili in maniera oggettiva: nel processo di valutazione, specialmente quando si valuta la performance rispetto agli obiettivi, le decisioni saranno supportate da analisi statistiche. Il punto di partenza è identificare quali aree misurare e, conseguentemente, definire alcuni indicatori rilevanti per misurarle (KPI). L'indicatore deve essere in qualche modo quantitativo, e quindi sarà spesso descritto in termini di valore numerico. Di seguito si riporta qualche esempio di KPI che la NewCo fornirà:

- numero di indicatori di compromissione (IoC) condivisi;
- numero di *white paper* pubblicati e numero di volte in cui sono stati scaricati;
- numero di presentazioni dell'ISAC a convegni esterni;
- numero di attività completate in un piano annuale.

In ottica di *Information sharing,* Fastweb si è già dotata di una piattaforma di *Threat Intelligence* ed *Information Sharing*, con l'obiettivo di una continua valorizzazione e scambio degli indicatori in una rete di condivisione. Questa piattaforma verrà messa a disposizione e le informazioni ricavate saranno messe a fattor comune tanto per la condivisione di informazioni rilevanti con lo CSIRT Italia, quanto per la condivisione con altri CSIRT o ISAC interessati. La piattaforma ha contribuito a migliorare il rilevamento e la prevenzione degli attacchi informatici con un sistema di condivisione degli IoC rapido ed efficiente; integrare il nuovo sistema nei processi e nelle tecnologie esistenti di prevenzione, monitoraggio e gestione degli attacchi informatici; sviluppare un'architettura per la raccolta, gestione, valorizzazione e condivisione degli indicatori di compromissione sfruttando lo standard STIX/TAXII ed il *framework* MITRE ATT&CK. Il processo ed i flussi di informazione sono descritti nell'immagine seguente:

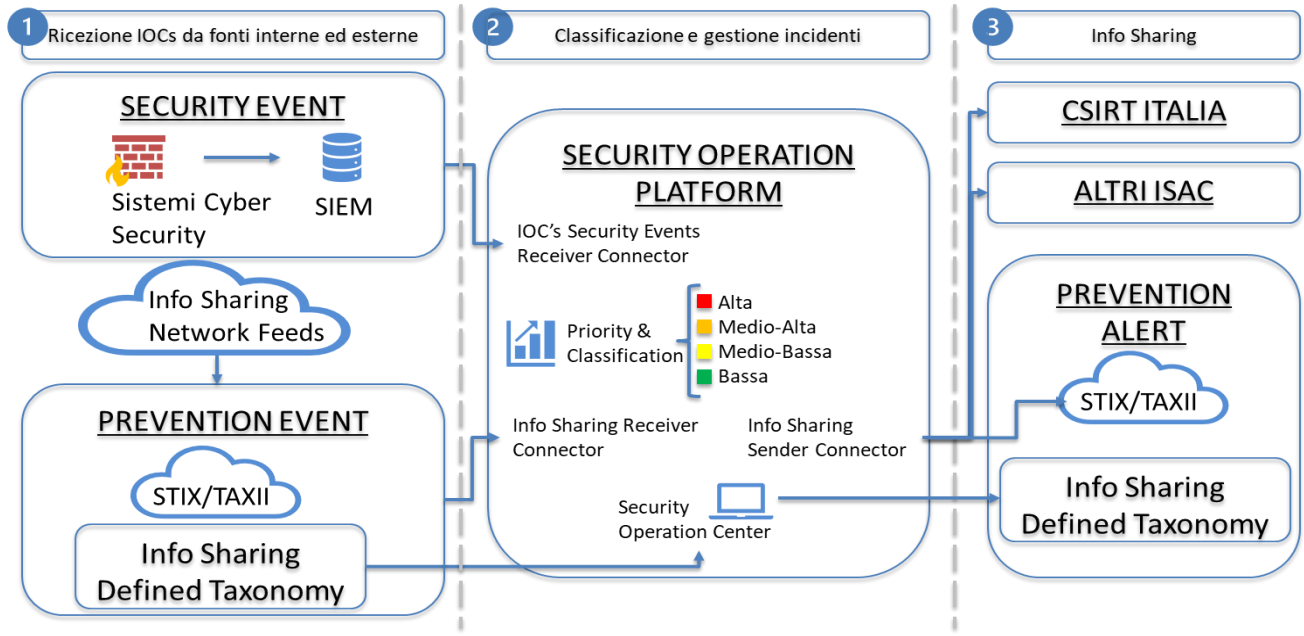



*Figura 35: Flussi informativi degli indicatori di compromissione*

Inoltre, le *capability* di Fastweb relative a *Threat Intelligence* ed *information sharing* comprendono i seguenti elementi:

- piattaforma di *intelligence* sulle minacce per la raccolta, la condivisione, l'archiviazione e la correlazione di indicatori di compromissione;
- strumento per la raccolta degli indicatori di compromissione in formato STIX;
- strumento per l'elaborazione, la deduplica e la normalizzazione degli indicatori di compromissione;
- SIEM per la risposta, l'analisi e la correlazione degli eventi notevoli aventi una corrispondenza con gli IoC, come descritto nell'immagine seguente a titolo di esempio.

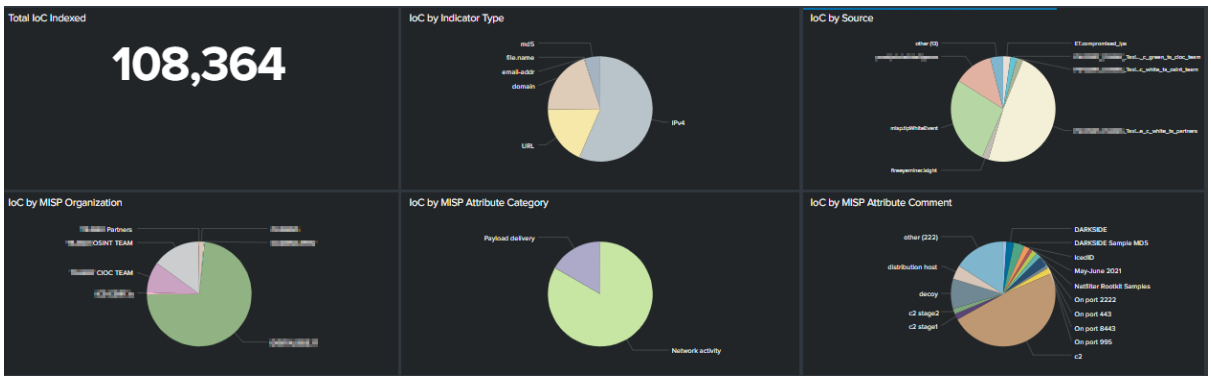



*Figura 36: Analisi eventi notevoli*

- piattaforma SOAR per l'automazione, la standardizzazione e l'integrazione con gli strumenti di sicurezza in uso;
- piattaforme che consentono di "consumare" e organizzare indicatori di compromissione ed altre informazioni sulle minacce *cyber*;

- piattaforma SIR per la collaborazione, l'elaborazione e la gestione di eventi di sicurezza;
- valorizzazione degli indicatori di compromissione a protezione dei presidi di sicurezza di tipo *Mail*, *Network* ed *Endpoint* anche tramite la collaborazione con il CNAIPIC.

In questo contesto, l'ecosistema degli indicatori di compromissione si presenta come una rete complessa e valorizzata da più fonti diverse:

- Fastweb CSIRT *Threat Hunting*;
- fonti OSINT;
- *feed* Pubblici (per esempio, Abuse.ch, AlienVault, DigitalSide, CyberCrime Tracker);
- *feed* Commerciali;
- *Constituency Information Sharing* come CNAIPIC e CSIRT Italia.

### 1.19.7 Interazioni con altri ISAC

Una volta valutate ed individuate le modalità di condivisione e le informazioni da scambiare all'interno dell'ISAC di settore proposto dalla NewCo, si passa ad una fase di valorizzazione e sviluppo ulteriore: in ottica di miglioramento continuo *dell'information sharing* descritto nei capitoli precedenti, la NewCo si propone di individuare e trattare nuovi tipi di informazioni da condividere, meccanismi di scambio, nuovi *stakeholder* o membri con cui collaborare, avviare un flusso di lavoro, organizzare una formazione o decidere attività di sensibilizzazione.
I risultati della valutazione e l'accordo sul potenziamento dell'ISAC fungeranno da base per il miglioramento effettivo degli aspetti operativi di quest'ultimo. Questa è la fase in cui i membri si incontrano, discutono e, in un ambiente creativo, propongono misure concrete per migliorare processi, *routine*, strumenti, cooperazione e, non ultima, la qualità dello scambio di informazioni. Questo esercizio porta al coinvolgimento di nuovi *stakeholder* e, in particolare, la NewCo in qualità di ISAC di settore si propone di farsi promotrice di incontri volti allo scambio di informazioni anche con ISAC di settore diversi dal proprio, andando ad aggiungere valore al proprio *know-how* ed arricchendo la rete di scambio con azioni concrete.
La NewCo si impegna fin da subito in attività di sensibilizzazione al fine di rendere le parti interessate consapevoli dell'attuale situazione della sicurezza, ad esempio minacce e vulnerabilità attuali ed emergenti. In tal modo, la conoscenza sarà diffusa al di fuori dell'ISAC e contribuirà alla sicurezza del settore e della società. Questo obiettivo sarà raggiunto, per esempio, attraverso la pubblicazione di articoli, *white paper* ed altre forme di informazioni pertinenti rese accessibili dall'ISAC stesso. L'ISAC di settore costituito dalla NewCo si pone l'obiettivo, inoltre, di svolgere un ruolo di consulenza, consigliando anche altre organizzazioni o altri ISAC su temi rilevanti o persino supportare le *start-up* con conoscenze specialistiche.
La creazione di un ecosistema ISAC sosterrebbe, così, l'incremento delle competenze e capacità di sicurezza in Europa, così come previsto da diversi Stati membri e dal settore privato. Gli ISAC perseguono anche l'obiettivo di costituire uno strumento utile nell'attuazione della Direttiva NIS, poiché offrono un "livello intermedio" tra gli operatori dei servizi essenziali ed i CSIRT a livello nazionale. Raccogliendo informazioni su minacce ed incidenti e supportando i propri membri nell'analisi di vulnerabilità e minacce, l'ISAC proposto dalla NewCo contribuirà in modo significativo al processo di gestione del rischio a livello nazionale ed internazionale.

### 1.19.8 *High Performance Computing* e simulazione tramite intelligenza artificiale e *Machine Learning*

La NewCo, nell'ambito del suo modello di servizio, potrà integrare infrastrutture di *High Performance Computing* (HPC) che:

- saranno rese disponibili alle PA utenti per l'erogazione dei servizi informatici verso i cittadini;

- serviranno come strumenti di analisi, valutazione e modellazione degli eventi di sicurezza.

Attraverso la modellazione degli eventi di sicurezza, sarà possibile integrare sorgenti di natura diversa grazie alla visibilità del PSN stesso (eventi di sicurezza associati alle PA utenti) e di Fastweb, che è in grado di raccogliere telemetrie riferite ai suoi clienti (PA, aziende, privati), dati associati ai servizi corporate, nonché quelli derivanti dai servizi di threat hunting e threat intelligence descritti nelle rispettive sezioni. La correlazione di una tale quantità di dati richiede tecnologie adeguate e capacità computazionale elevata per poter eseguire analisi complesse in tempi rapidi in modo da poter determinare tempestivamente le azioni di risposta a potenziali eventi di sicurezza. Attraverso le capacità di *High Performance Computing,* il PSN potrà sviluppare modelli che prendono in considerazione:

- tattiche e Procedure (TTP) di attacco innovative, al fine di identificare tempestivamente nuove modalità di attacco;
- analisi degli Indicatori di Compromissione (IoC) derivanti dalla gestione di eventi ed incidenti di sicurezza rilevati dal PSN e da Fastweb;
- vulnerabilità presenti nell'infrastruttura, loro esposizione e rischi associati al contesto in cui si verificano, al fine di definire un percorso di *patching* prioritizzato;
- sistemi ed *asset* critici, anche in linea con quanto definito all'interno della Direttiva NIS e del PSNC;
- analisi delle diverse azioni di mitigazione e dei controlli compensativi in presenza di rischi di sicurezza.

Il PSN potrà implementare tale modello attraverso strumenti e tecnologie già presenti sul mercato, o attraverso la realizzazione di strumenti di analisi sviluppati *ad hoc* mediante funzionalità di AI e *machine learning* in grado di sfruttare al meglio le capacità dell'architettura HPC.

Il processo viene descritto nell'immagine seguente:

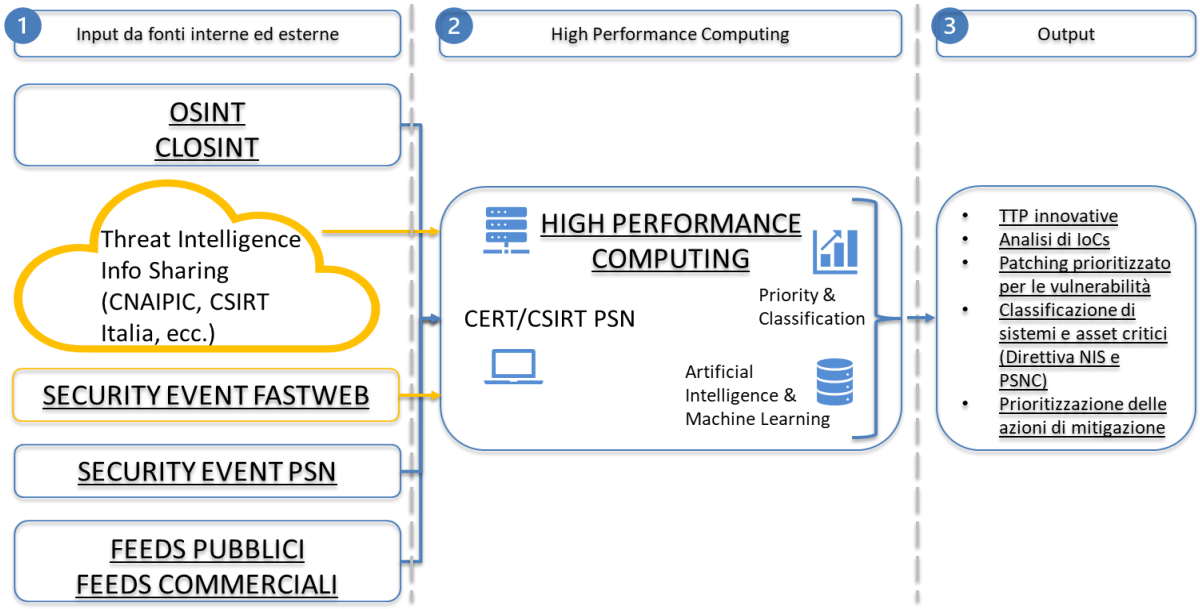



*Figura 37: Processo di elaborazione dell'architettura HPC*

Le informazioni raccolte e ottenute attraverso questo modello potranno poi essere condivise con il CSIRT Italia e gli ISAC secondo quanto descritto nel paragrafo "*Interazione con l'ISAC e CSIRT Italia*".

### 1.19.9 Fastweb *Digital Academy*

La NewCo PSN metterà a disposizione della Pubblica Amministrazione il proprio *know-how* in termini di formazione in *cyber security*, con l'obiettivo di creare entro il 2022 l'infrastruttura per il PSNC in collaborazione con l'Agenzia Nazionale per la Cybersicurezza, al fine di sostenere lo sviluppo delle imprese di *cybersecurity* in Italia, compreso lo *scale-up* delle PMI e delle *start-up* esistenti.
Attualmente, Fastweb eroga servizi di formazione in tale ambito tramite la scuola per le nuove competenze digitali (Fastweb *Digital Academy*) creata dalla stessa Fastweb insieme a Fondazione Cariplo. Inoltre, Fastweb è uno dei soggetti che hanno risposto alla richiesta di proposte di formazione da parte della Funzione Pubblica. I percorsi della Fastweb *Digital Academy* sono dedicati alla formazione ed al perfezionamento delle professionalità più ricercate nell'ambito della sicurezza informatica, come il *Network Security Architect* ed il *Cyber Analyst*. La Fastweb *Digital Academy* prevede la formazione attraverso sessioni formative basate su scenari reali, predisposti attraverso una piattaforma dedicata resa disponibile a tutti i partecipanti alle attività di *awareness*.

Inoltre, Fastweb Digital Academy, in collaborazione con ASC Aps, ha aderito all'iniziativa "*Ponti digitali per reti sociali*", il Programma quadro di sperimentazione del Servizio Civile Digitale promosso dal Dipartimento per la trasformazione digitale ed il Dipartimento per le politiche giovanili ed il servizio civile universale della Presidenza del Consiglio dei Ministri. L'iniziativa ha lo scopo di contribuire a superare l'attuale *gap* sulle competenze digitali e di produrre un benefico specifico impatto sulle comunità, in linea con quanto delineato dal PNRR e nella Strategia nazionale per le competenze digitali, per i quali viene reputato fondamentale lo sviluppo ed il potenziamento dei servizi di "*facilitazione digitale*" sul territorio. Sfruttando le competenze acquisite nella programmazione ed attuazione dei programmi e progetti di Servizio Civile Universale, ASC Aps ha contribuito all'iniziativa coinvolgendo 27 enti di accoglienza in 11 Regioni per raggiungere fasce di popolazione oggi in difficoltà nell'utilizzo degli strumenti digitali, accompagnando i giovani nelle attività a favore dei cittadini e rendicontando l'impatto degli interventi.
Fastweb, attraverso la Fastweb *Digital Academy*, ha messo a disposizione degli operatori volontari selezionati da ASC Aps il *test* delle competenze digitali *Digital* IQ e percorsi di formazione, tra cui uno dedicato alla Sicurezza in rete e uno focalizzato sul *Personal Branding*, per fornire, oltre agli strumenti tecnici, anche la necessaria consapevolezza rispetto non solo ai rischi, ma anche alle opportunità che il digitale può offrire.
Dal 2016 a oggi, Fastweb *Digital Academy* ha rilasciato oltre 12.000 certificati, organizzando 430 classi per un totale di 9750 ore di formazione erogate a sostegno di giovani, studenti e piccole e medie imprese. L'impegno costante di Fastweb a favore della sostenibilità sociale e dell'alfabetizzazione digitale del Paese si inserisce all'interno di NeXXt Generation 2025, il piano annunciato da Fastweb a dicembre 2021 con l'obiettivo di connettere con il futuro milioni di famiglie sul territorio nazionale contribuendo a fornire le necessarie competenze digitali. Attraverso Fastweb *Digital Academy* l'azienda punta a rilasciare 50.000 certificati entro il 2025.
La NewCo PSN fornirà quindi alle PA utenti, in partnership con la Fastweb *Digital Academy*, formazione ed *awareness* sui temi di sicurezza informatica, sia attraverso una formazione di carattere generale sia tramite una formazione per gli utenti specializzati in IT e *Cyber Security*.

### *1.19.10 Tech Screening Network*

La NewCo, nell'ambito delle attività previste, assicura pieno supporto alle PA utenti chiamate anche a collaborare con il CVCN (Centro di Valutazione e Certificazione Nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia) e con i CV istituiti presso il Ministero dell'interno ed il Ministero della difesa, in tutte le attività

funzionali alle verifiche preliminari ed ai test *hardware* e *software* su beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1 comma 2 lett. b) della L. 133/2019. Su richiesta della PA utente, la NewCo mette a disposizione il proprio *know-how*, le risorse fisiche (per esempio, componenti accessori, realizzazione di *test bed*), le risorse logistiche (per esempio, messa a disposizione di sedi idonee all'effettuazione dei *test* su richiesta della PA utente) e professionali, ovvero figure in grado di fornire il necessario supporto alle PA utenti, sia nella fase che precede l'effettuazione dei test, che durante la loro esecuzione, nonché successivamente, per la produzione dell'eventuale documentazione tecnico - amministrativa necessaria.
A tal proposito, Fastweb, grazie alle numerose convenzioni ed Accordi Quadro Consip di cui è aggiudicataria, vanta un *network* di laboratori di sicurezza attrezzati ed equipaggiati con tecnologie e dispositivi all'avanguardia, che consentono l'analisi approfondita di apparati *embedded*, con il fine di individuare possibili problematiche di sicurezza. In particolare, si è dotata di locali tecnici, infrastrutture, strumentazioni di *test* e misura, centri di gestione, risorse specializzate e processi dedicati all'effettuazione di collaudi e di prove tecniche volti alla certificazione di servizi e prodotti di sicurezza dedicati alla PA, secondo le specifiche Consip.
Pertanto, attraverso la completa supervisione degli specialisti interni, Fastweb è in grado di supportare le PA nella verifica della conformità dei test effettuati dai CVCN e CV. Questo si concretizza con il consolidamento dei requisiti, la redazione della documentazione di collaudo, l'individuazione dei test necessari a verificare i requisiti, il *tuning* dell'ambiente di prova, il supporto alle commissioni di collaudo, l'effettuazione dei *test* e la documentazione degli esiti degli stessi. Per l'esecuzione dei *test*, Fastweb sfruttando gli accordi di *partnership* che garantiscono il massimo supporto nello svolgimento delle attività, può assicurare anche l'apertura di tavoli tecnici con il coinvolgimento del *vendor* della tecnologia specifica per assicurare un confronto tempestivo in caso di necessità.
Il PSN, attraverso l'erogazione dei servizi CERT relativi alla "*product evaluation and certification*" rappresenterà un punto di riferimento per tutte le PA che volessero valutare e certificare i propri prodotti *software* o *hardware* da un punto di vista della sicurezza. Inoltre, enti come l'AgID potranno avvalersi dei servizi erogati dalla NewCo per l'identificazione e l'inserimento in un catalogo *ad hoc* degli strumenti certificati nel rispetto dei requisiti di sicurezza imposti.

### *1.19.11 National HyperSOC*

La NewCo PSN, si propone di attestarsi come uno dei 5 centri operativi di sicurezza nazionale da integrare con quello centrale, con l'obiettivo di rafforzare le strutture operative chiave del PSNC e, più precisamente, in riferimento all'obiettivo dell'istituzione di un «*National hyper* SOC» (centrale), previsto entro il 2023, per il monitoraggio e l'elaborazione di eventi sospetti che hanno luogo all'interno del PSNC stesso.
Con questo obiettivo, il SOC dovrà basarsi su un *framework* architetturale, allineato agli *standard* di riferimento quali il NIST *Cybersecurity Framework*, ed essere composto da tecnologie, processi e risorse professionali specializzate, come già avviene per quello di Fastweb. A tal proposito, è importante sottolineare come l'apparato SOC-CSIRT di Fastweb sia in grado di controllare ed analizzare gli eventi relativi al PSN, integrandone ed espandendone le funzionalità intrinseche.
Il *framework* proposto si basa su tecnologie all'avanguardia e si avvale di strumenti *leader* di mercato in grado di migliorare:

- la qualità delle informazioni raccolte e la relativa indicizzazione e correlazione;
- la capacità di rilevamento delle minacce attraverso un *tuning* puntuale, l'adozione dei moduli di *Behavioural Analytics* e di *Anomaly Detection,* a complemento delle funzioni *core* di una soluzione di *log collection* e *correlation* (per esempio, SIEM);
- le investigazioni e le analisi di nuove minacce, coadiuvate da specifiche soluzioni di *Threat Intelligence* e di *Information sharing*, così come descritte nei capitoli dedicati;

- l'automazione della gestione degli eventi di sicurezza e degli incidenti integrando le fonti informative e le tecniche di risposta in modo che tutte le PA possano beneficiarne, anche se non direttamente impattate dagli attacchi rilevati.

Le *capability dell'HyperSOC* Nazionale così definito si baseranno su:

- visibilità di eventi di sicurezza e minacce emergenti da parte di Fastweb e della NewCo;
- sfruttamento delle capacità computazionali messe a disposizione *dall'High Performance Computing* descritto in precedenza.

### 1.19.12 Supporto alle PA utenti

Nell'ambito del supporto alle PA utenti, la NewCo mette a disposizione il proprio *know-how* in termini di formazione in *cyber security* attraverso diverse iniziative. La NewCo si avvarrà delle significative esperienze di collaborazione con le PA e dell'approfondita conoscenza delle loro esigenze e specificità che Fastweb ha maturato grazie alle numerose convenzioni Consip, in particolare la convenzione sulla *cybersecurity* SPC *Cloud* Lotto 2 Sicurezza, SPC 2CONN ed agli Accordi Quadro di cui è aggiudicataria in ambito *cybersecurity*, tra cui quelli con ID 2174 ed iD 2296.
Oltre alla collaborazione con la già citata Fastweb *Digital Academy* (FDA), l'Offerente propone la creazione di un "*cyber range*" per l'addestramento del personale incaricato della gestione e reazione agli attacchi nell'ambito del PSN, per una *partnership* che vede coinvolti anche altri attori: Fastweb stessa, la controllata 7Layers e diverse università, tra cui Politecnico di Milano, Università di Bologna, Università di Modena e Reggio Emilia. Questa *Security Academy* nasce con l'obiettivo di formare figure specializzate in *Cybersecurity* per soddisfare esigenze aziendali, del mercato, ed in generale per la diffusione delle competenze digitali.

La *Security Academy* prevede la formazione di figure specializzate in *Cybersecurity* (livello *Security Architect*/*Cybersecurity Analyst*) attraverso un percorso dedicato da sviluppare in sinergia con la FDA. Il percorso formativo prevede 2 corsi da erogare su personale pre-qualificato (tramite test d'ingresso) con docenti di livello universitario. In particolare:

- corso BASE (1 docente per 20 ore) con l'obiettivo di uniformare il livello dei partecipanti;
- corso AVANZATO (2 docenti per 60 ore) con l'obiettivo di erogare i contenuti specifici di *Cybersecurity*.

Tutto il *know-how* derivante dalla formazione erogata attraverso questa molteplicità di iniziative verrà messo a disposizione delle PA utenti e delle imprese incluse nel PSNC e nel NIS. Le competenze costituiranno, per dette organizzazioni, un incentivo all'introduzione di nuove capacità di *cyber security*, a sostegno del rafforzamento della sicurezza informatica nelle strutture operative chiave del PSNC, del NIS, ed in generale nel settore della *cyber defense* e *law enforcement*.

### 1.19.13 CERT e CSIRT

La NewCo realizzerà e metterà a disposizione delle PA utenti una struttura CERT/CSIRT responsabile dell'erogazione dei servizi di gestione proattiva e reattiva dei servizi di sicurezza. Tale struttura, beneficerà anche di tutte le informazioni raccolte da Fastweb nell'ambito del monitoraggio dei propri clienti (privati, imprese, PA), nonché delle informazioni raccolte dal CERT *Corporate* di Fastweb. Questa visibilità estesa permetterà di raccogliere un elevato numero di informazioni su eventi di sicurezza che costituiranno un contributo chiave sia in ottica di servizi di sicurezza offerti alle PA, sia nell'ambito della condivisione di informazioni con altri ISAC supportando così le iniziative introdotte dal PNRR in ambito *cybersecurity*.
Inoltre, il CERT del PSN erogherà servizi di sicurezza a valore verso le PA, sia avvalendosi delle proprie risorse e competenze, sia appoggiandosi alle strutture di Fastweb che hanno una

consolidata esperienza in questo ambito, grazie all'erogazione di servizi di *cybersecurity* ai propri clienti *enterprise* ed ai clienti della PA (attraverso varie convenzioni Consip).

Le interazioni tra le varie strutture che partecipano all'erogazione dei servizi di sicurezza offerti sono rappresentate nella seguente immagine:

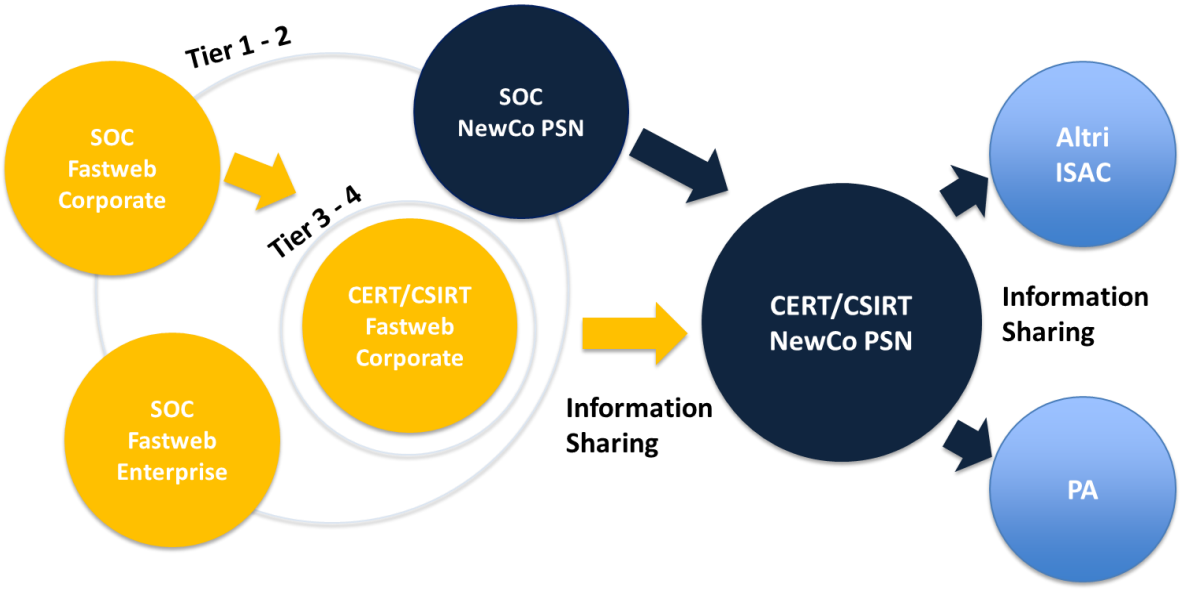



*Figura 38: Strutture che partecipano all'erogazione dei servizi di sicurezza*

### 1.19.14 Servizi erogati

I servizi erogati da un CERT possono essere raggruppati in tre categorie:

- servizi reattivi. Questi servizi vengono attivati da un evento o da una richiesta, ad esempio da un *report* di un *host* compromesso, da una diffusione di codice malevolo, da vulnerabilità del *software* o da qualsiasi altra anomalia identificata da un sistema di rilevamento delle intrusioni o di registrazione. I servizi reattivi sono la componente principale del lavoro di un CERT;
- servizi proattivi. Questi servizi forniscono assistenza ed informazioni per aiutare a preparare, proteggere i sistemi in *scope* in previsione di attacchi o eventi. Le prestazioni di questi servizi ridurranno direttamente il numero di incidenti in futuro;
- servizi di gestione della qualità della sicurezza. Questi servizi potenziano altri servizi già esistenti e ben consolidati, indipendenti dalla gestione degli incidenti e tradizionalmente eseguiti da altre unità di un'organizzazione come i dipartimenti IT, *audit* o formazione. Se il CERT svolge o assiste questi servizi, il punto di vista e le competenze dello stesso CERT possono fornire informazioni utili per migliorare la sicurezza generale dell'organizzazione ed identificare rischi, minacce e debolezze del sistema. Questi servizi sono generalmente proattivi ma contribuiscono indirettamente alla riduzione del numero di incidenti.

I servizi erogati per ogni categoria vengono riportati nell'immagine seguente:

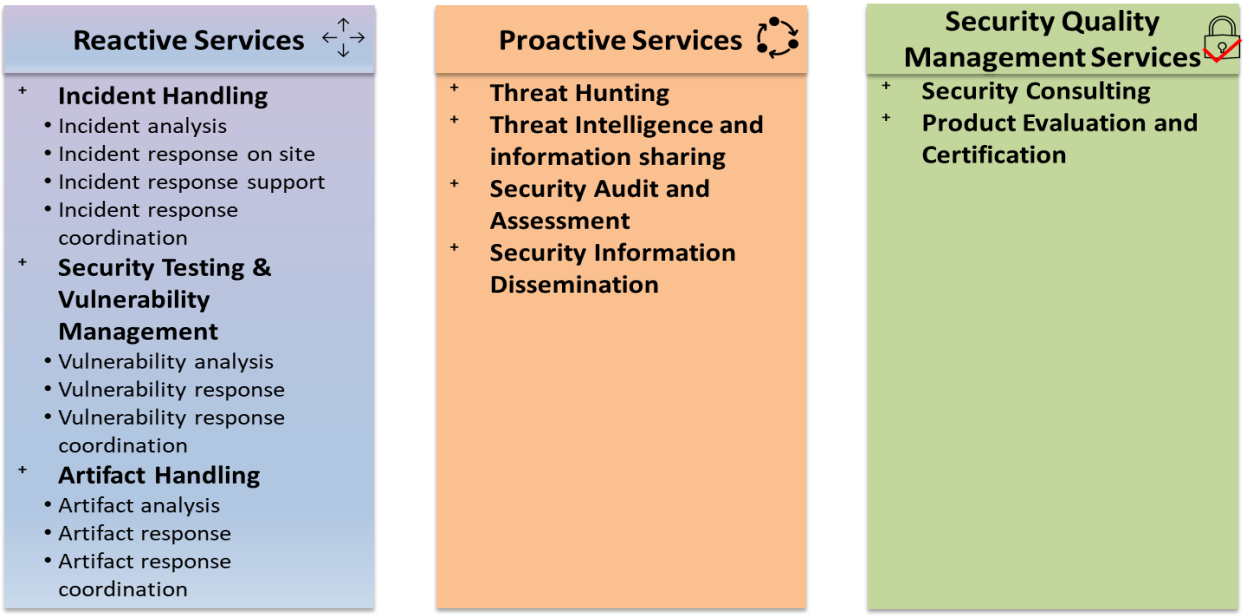



*Figura 39: Categorie servizi erogati da un CERT*

La NewCo costituirà un CERT dal quale saranno erogati i servizi di sicurezza reattivi e proattivi. La *control room* del CERT sarà localizzata esternamente ai DC del PSN. Le componenti tecniche che implementano i controlli tecnologici che proteggono le infrastrutture a supporto dei servizi saranno, invece, ospitate all'interno dei DC. I servizi CERT saranno disponibili in modalità 7x24.

### *1.19.15 Threat Hunting*

Il CERT monitora continuamente la propria infrastruttura e le fonti di intelligence (sia OSINT che CLOSINT) per rilevare potenziali vettori di attacco o indicatori associabili alla compromissione delle infrastrutture, degli ambienti elaborativi, per indentificare comportamenti anomali o associabili a tecniche e modalità di attacco note. In quest'ottica la NewCo attraverso i servizi CERT monitorerà la propria infrastruttura e gli *asset* gestiti per conto delle PA utenti, al fine di identificare potenziali scenari di attacco e reagire proattivamente per renderli inefficaci, o comunque per mitigarne gli impatti. Inoltre, le informazioni raccolte in questo ambito saranno condivise con gli altri ISAC attraverso i servizi descritti nella sezione successiva, relativa a *threat intelligence* ed *information sharing*.

### *1.19.16 Threat Intelligence ed Information Sharing*

La NewCo sfrutterà servizi avanzati di *threat intelligence* & *information sharing* e adotterà strumenti, procedure e personale per assicurare competenze predittive in ambito sicurezza cibernetica.
Nel farlo, verranno attivati servizi di *intelligence* che consentano di:

- scambiare informazioni opzionalmente anonimizzate su nuove tecniche di attacco (TTP) e scenari di minaccia;
- scambiare informazioni opzionalmente anonimizzate, anche in forma di IoC su incidenti di sicurezza cibernetica;
- ricevere notifiche ed allarmi su minacce (per esempio, *zero-day*, campagne di *malware*, pandemie digitali, attori ed incidenti).

Per verificare in maniera capillare e tempestiva la presenza di indicatori di compromissione, il PSN si doterà di strumenti di IoC *automation* basati sull'integrazione di:

- piattaforme *Open Source* (per esempio, MISP *Open Source Threat Intelligence and Sharing Platform*);

- *software* di protezione avanzata denominato *Endpoint Detection & Response*;
- strumenti di *Log Management & Correlation* in grado di correlare ed allarmare la presenza di IoC sia in *real-time* che sullo storico dei *log* con congrua profondità.

Anche nell'ambito della *Threat Intelligence* la NewCo si doterà dei servizi di *information sharing* descritti nei capitoli dedicati all'ISAC ed alle sue interazioni, avendo essi un ruolo chiave nella condivisione tempestiva di nuove informazioni legate a possibili scenari di attacco.

### *1.19.17 Security testing & Vulnerability Management*

La gestione delle vulnerabilità implica la ricezione di informazioni e rapporti su vulnerabilità di *hardware* e *software*; analizzarne la natura e gli effetti; sviluppare strategie di risposta per rilevarle e per fare attività di *remediation*. La NewCo avrà a disposizione strumenti, procedure e personale per gestire le attività di *testing* delle infrastrutture, valutarne i relativi risultati, identificare ed indirizzare le strategie di mitigazione. Nello specifico le attività saranno suddivise come segue:

- *vulnerability analysis*: prevede l'analisi tecnica e l'esame di vulnerabilità *hardware* o *software*. Ciò include la verifica della vulnerabilità sospetta e l'esame tecnico della stessa per determinare dove si trova e come può essere sfruttata. L'analisi può includere l'attività di revisione del codice sorgente, l'utilizzo di un *debugger* per determinare dove si verifica la vulnerabilità o la riproduzione della vulnerabilità su un sistema di *test*. Al fine di rimediare le vulnerabilità riscontrate, la NewCo adotterà le procedure di gestione delle vulnerabilità in linea con le *best practice* di settore ed i principali standard di sicurezza (per esempio, CIS, SANS, PCI DSS). Le stesse prevedono che la classificazione delle vulnerabilità avvenga secondo *standard* internazionali (per esempio, CVSS) e gli interventi di correzione o mitigazione siano proporzionati al livello di esposizione al rischio introdotto dalle vulnerabilità;
- *vulnerability response*: comporta la determinazione della risposta appropriata a mitigare una vulnerabilità. Ciò può comportare lo sviluppo o la ricerca di *patch*, correzioni e soluzioni alternative. Implica anche la notifica ad altri della strategia di mitigazione, eventualmente con la creazione e distribuzione di avvisi tramite rete di *information sharing*;
- *vulnerability response coordination*: comprende la notifica e la condivisione con le varie parti interessate di informazioni su come correggere o mitigare la vulnerabilità. Comprende anche la verifica che la strategia di risposta alla vulnerabilità sia stata implementata con successo. Questa attività può comportare la comunicazione con i fornitori, altri CSIRT, esperti tecnici, membri costituenti e le persone o i gruppi che inizialmente hanno scoperto o segnalato la vulnerabilità, sempre in ottica di *information sharing*.

### *1.19.18 Incident Response*

La NewCo assicurerà la gestione degli incidenti, che include la ricezione, il *triage* e la risposta a richieste e segnalazioni, oltre all'analisi di incidenti ed eventi. Le attività di risposta possono includere:

- azioni per proteggere i sistemi e le reti colpiti o minacciati da attività di intrusi;
- soluzioni e strategie di mitigazione;
- ricerca di attività di intrusi all'interno dell'intera infrastruttura;
- filtraggio del traffico di rete;
- ripristino dei sistemi;
- *patching* dei sistemi;
- altre strategie di risposta o soluzioni alternative.

Il servizio è ulteriormente classificato, in base al tipo di attività svolta ed al tipo di assistenza fornita, come segue:

*Incident analysis*. Si tratta di un esame di tutte le informazioni disponibili comprese le evidenze o gli artefatti relativi a un incidente o evento. Lo scopo dell'analisi è identificare la portata dell'incidente, l'entità del danno causato dall'incidente, la natura dell'incidente e le strategie di risposta disponibili o soluzioni alternative. I risultati di analisi delle vulnerabilità ed analisi degli artefatti (descritti in altri paragrafi) possono essere usati per comprendere e fornire un'analisi completa ed aggiornata di ciò che è accaduto su uno specifico sistema. Il CERT correla gli indicatori di diversi incidenti per determinare eventuali interrelazioni, tendenze, modelli o le tracce caratteristiche lasciate da ciascun intruso. A seconda degli obiettivi e dei processi prefissati come parte dell'analisi degli incidenti, possono essere eseguiti due sottoservizi:

- raccolta di prove forensi: la raccolta, la conservazione, la documentazione e l'analisi di prove da un sistema informatico compromesso per determinare le modifiche avvenute e per assistere nella ricostruzione degli eventi che hanno portato alla compromissione. Questa raccolta di informazioni e di prove deve essere fatta in modo da documentare una catena dimostrabile di custodia ammissibile in un tribunale. Compiti coinvolti nella raccolta di prove forensi includono la creazione di una copia *bit-image* del disco rigido del sistema interessato; la verifica di modifiche al sistema come nuovi programmi, *file*, servizi e utenti; l'esame dei processi in esecuzione e delle porte di rete aperte; il controllo di *Trojan horse* e *rootkit*;
- tracciamento: l'identificazione di sistemi a cui l'intruso ha avuto accesso. Questa attività potrebbe comportare il monitoraggio o il tracciamento di come l'intruso sia entrato nei sistemi interessati e nelle reti, quali sistemi abbia utilizzato per ottenere l'accesso, dove abbia avuto origine l'attacco e quali altri sistemi e reti siano stati utilizzati come parte dell'attacco. Potrebbe anche comportare il tentativo di determinare l'identità dell'intruso. Questo lavoro può essere svolto dal CERT in autonomia, ma, di solito, comporta il lavoro congiunto con il personale delle forze dell'ordine, i fornitori di servizi Internet o altre organizzazioni coinvolte.

*Incident response on site*. Il CERT fornisce assistenza diretta *in loco* per supportare il ripristino di sistemi, dati e operatività a seguito di un incidente. Essa comprende l'analisi fisica dei sistemi colpiti e la riparazione ed il ripristino degli stessi, anziché un semplice supporto da remoto. Questo servizio comprende tutte le azioni a livello locale che sono necessarie durante le fasi di verifica di un incidente.

*Incident response support*. Il CERT assiste e guida la vittima nella gestione dell'incidente tramite telefono, *e-mail* o documentazione. Questo può comprendere assistenza tecnica nell'interpretazione dei dati raccolti, fornendo informazioni di contatto, o trasmissione di linee guida sulle strategie di mitigazione e ripristino. Non coinvolge direttamente, *in loco*, azioni di risposta agli incidenti come descritto sopra. Il CERT, invece, fornisce indicazioni da remoto in modo che il personale del sito possa eseguire il ripristino in autonomia.

*Incident response coordination*. Il CERT coordina le attività di risposta tra le parti coinvolte nell'incidente. Generalmente, sono coinvolti nell'analisi la vittima dell'attacco ed i vari *stakeholder*. Può anche includere le parti che forniscono supporto informatico alla vittima, come i fornitori di servizi *Internet*, altri CERT ed amministratori di sistema e di rete del sito. Il lavoro di coordinamento può implicare la raccolta di informazioni di contatto, la notifica ai siti del loro potenziale coinvolgimento (per esempio, vittima o fonte di un attacco), raccogliendo statistiche sul numero di siti coinvolti e facilitando lo scambio e l'analisi delle informazioni. Parte del lavoro di coordinamento può includere la notifica e la collaborazione con: il consulente legale di un'organizzazione, le risorse umane e le forze dell'ordine laddove necessario. Questo servizio non prevede una risposta diretta agli incidenti *in loco*.

### 1.19.19 Artifact handling

Un artefatto è qualsiasi *file* trovato su un sistema che potrebbe essere coinvolto nelle ricognizioni o negli attacchi a sistemi e reti o che può essere utilizzato per aggirare le misure di sicurezza. Artefatti possono includere, a titolo esemplificativo, *virus* informatici, *Trojan*, *worms*, *exploit script* e *rootkit*.
La gestione degli artefatti prevede la ricezione di informazioni e copie degli artefatti che vengono utilizzati in attacchi esterni, ricognizioni ed altre attività non autorizzate o di disturbo. Una volta ricevuto, l'artefatto viene rivisto. Ciò include l'analisi della natura, della meccanica, della versione e dell'utilizzo degli artefatti, oltre a sviluppare (o suggerire) strategie di risposta per rilevare, rimuovere e difendersi da tali artefatti. Questo servizio sarà orientato all'analisi degli eventi ed all'identificazione di eventuali nuovi IoC relativi ad attacchi non noti, con l'obiettivo di proteggere in maniera proattiva le PA utenti e fornire servizi di *information sharing* verso altri CERT/CSIRT, nonché verso gli ISAC.
Il servizio verrà implementato in diversi *stream*, categorizzati sulla base delle attività dedicate ad ognuno di essi, come segue:

- *artifact analysis*: lo CSIRT esegue un esame tecnico e l'analisi di qualsiasi artefatto trovato su un sistema. L'analisi effettuata potrebbe includere l'identificazione del tipo di file e della struttura dello stesso, confrontando un nuovo artefatto con artefatti esistenti o altre versioni dello stesso artefatto per rilevare somiglianze e differenze, e svolgendo attività di *reverse engineering* per determinarne lo scopo e la funzione;
- *artifact response*: questa attività comporta la determinazione delle azioni necessarie a rilevare e rimuovere artefatti da un sistema, nonché per impedirne l'installazione;
- *artifact response coordination*: questa attività prevede la condivisione e la rappresentazione dei risultati e delle strategie di risposta relative a un artefatto con altri ricercatori, CSIRT, fornitori ed altri esperti di sicurezza. Le attività possono anche includere il mantenimento di un archivio pubblico di artefatti noti ed il loro impatto con la corrispondente strategia di risposta.

### 1.19.20 Security Information Dissemination

L'Offerente propone un servizio di "*security information dissemination*" con lo scopo di fornire al perimetro PSN una raccolta completa di informazioni utili che aiutano a migliorare la sicurezza. Questa *knowledge base* sarà integrata dalle rilevazioni eseguite da Fastweb sulle minacce ed eventi di sicurezza relativi ai propri clienti. Le informazioni oggetto della condivisione includono:

- linee guida di segnalazione ed informazioni di contatto per il CERT;
- archivi di *alert*, *warning* ed altri annunci;
- documentazione sulle *best practice*;
- indicazioni generali sulla sicurezza informatica;
- *policy*, procedure e *checklist*;
- informazioni sullo sviluppo e sulla distribuzione delle *patch*;
- collegamenti con i fornitori;
- statistiche e tendenze attuali nella segnalazione degli incidenti;
- altre informazioni che possono migliorare le pratiche di sicurezza generali.

### 1.19.21 Security Consulting

L'Offerente propone di utilizzare il CERT per fornire consigli ed indicazioni sulle migliori *best practice* di sicurezza alle PA utenti. In particolare, il servizio è rivolto a tutti i clienti del PSN nella gestione delle esigenze di *security operation*, ma anche per la definizione di nuove iniziative

progettuali, nonché di analisi dei rischi e valutazioni di impatti derivanti da nuove iniziative in ambito IT o da nuove minacce di sicurezza.
Un CERT che fornisce questo servizio è coinvolto nella preparazione di raccomandazioni o nell'identificazione dei requisiti per l'acquisto, l'installazione e protezione di nuovi sistemi, dispositivi di rete, *software* o processi per altre attività a livello aziendale. Questo servizio include la guida e l'assistenza nella stesura di politiche di sicurezza.

### *1.19.22 Security Audit/Assessment*

Al fine di monitorare lo stato di implementazione della sicurezza all'interno del PSN, ma anche per il monitoraggio delle terze parti e della *supply chain*, l'Offerente propone di fornire un servizio di *security audit* ed *assessment*.
Questo servizio fornisce una revisione e un'analisi dettagliate della sicurezza dell'infrastruttura di un'azienda, in base ai requisiti definiti dalle PA utenti o da altri *standard* di settore applicabili. Può anche comportare una revisione delle pratiche di sicurezza dell'organizzazione.
Diversi tipi di *audit* o *assessment* possono essere effettuati verso le terze parti coinvolte, tra cui:

- *Infrastructure review*: revisione manuale delle configurazioni *hardware* e *software*, router, *firewall*, *server* e dispositivi *desktop* per garantire che corrispondano a *best practice* e configurazioni *standard* dell'organizzazione o del settore;
- *Best practice review*: interviste a dipendenti ed amministratori di sistema e di rete per determinare se le loro procedure e prassi corrispondono alla *policy* di sicurezza organizzativa definita o agli standard di settore specifici;
- *Scanning*: utilizzo di scanner di vulnerabilità o *virus* per determinare quali sistemi e reti siano vulnerabili;
- *Penetration test*: testare la sicurezza di un sito attaccando di proposito i suoi sistemi e reti.

### *1.19.23 Product evaluation and certification*

Nell'ambito delle attività di valutazione e certificazione dei prodotti, il CERT svolge analisi volte a verificare la sicurezza dei prodotti e la loro conformità con gli obiettivi definiti dall'organizzazione. Tali attività, come descritto nella sezione *Tech Screening Network*, saranno svolte in collaborazione con il CVCN.
In quest'ottica, la NewCo svilupperà dei servizi *ad hoc* per la certificazione dei prodotti e degli strumenti utilizzati dalle PA seguendo due modalità:

- programma di valutazione: analisi e valutazione dei prodotti ritenuti di maggior interesse da parte del PSN rispetto a caratteristiche di innovazione, diffusione ed esposizione al rischio;
- *on-demand*: su richiesta delle PA, per casistiche specifiche e rilevanti.

Laddove possibile, sulla base degli *standard* disponibili, i prodotti, oltre a essere validati, saranno anche certificati rispetto a requisiti specifici (per esempio, requisiti AgID).

## 1.20 ID CRITERIO:20 – VALUTATIVO - COMPLETEZZA, ACCURATEZZA E VERIFICABILITÀ DEL METODO CHE IL CONCORRENTE SI IMPEGNA AD ADOTTARE PER LA DEFINIZIONE DEL DIMENSIONAMENTO DELLE RISORSE (GIORNI/UOMO E RELATIVO TEAM MIX PER TIPOLOGIA DI STRATEGIA DI MIGRAZIONE) E DELLE TEMPISTICHE PER LA REALIZZAZIONE DI CIASCUNA FASE DI CIASCUN PROGETTO DI MIGRAZIONE PER GLI SCENARI 1, 2 E 3 E PER I CASI DI "BREVE TERMINE" E "MEDIO E LUNGO TERMINE"

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 20 | Valutazione | Migrazione | Miglioramento delle modalità per la migrazione in *cloud* - Risorse e tempistiche | Completezza, accuratezza e verificabilità del metodo che il concorrente si impegna ad adottare per la definizione del dimensionamento delle risorse (giorni/uomo e relativo team mix per tipologia di strategia di migrazione) e delle tempistiche per la realizzazione di ciascuna fase di ciascun progetto di migrazione per gli scenari 1, 2 e 3 e per i casi di "breve termine" e "medio e lungo termine" | **5** |

Di seguito è descritto il **metodo** che l'Offerente si impegna ad adottare per il criterio 20, caratterizzato da **completezza, accuratezza e verificabilità** come richiesto nella descrizione del criterio stesso.
Infatti, a beneficio della **trasparenza e verificabilità** del metodo descritto in questa sezione, basato su *standard,* modelli e metodologie di provata efficacia, l'Offerente si impegna a utilizzare degli **strumenti a supporto delle migrazioni** (vedi capitolo 1.21) che offrono funzionalità per il dimensionamento di risorse e tempi delle migrazioni, e che l'Offerente si offre di:

- **rendere oggetto di possibili *audit* da parte del Concedente** (ove possibile, ad es. *tool* proprietari), per verificarne l'effettiva efficacia nel dimensionare correttamente le risorse in base al contesto ed alle necessità della PA utente;
- **rendere accessibili al Concedente** (ove possibile) per monitorare costantemente le risorse complessive impiegate dalle migrazioni.

### 1.20.1 Analisi del parco applicativo

La valutazione del parco applicativo si focalizza su quattro direttrici:

- la *cloud readiness* dell'applicativo;
- i requisiti funzionali e tecnici dell'applicativo;
- le dipendenze con la piattaforma ed il sistema operativo sottostante;
- le dipendenze con altri applicativi, *database ed* altri componenti.

Tale analisi si basa sulle principali sorgenti di informazione quali:

- il *Configuration Management Data Base* (CMDB) o eventuali altri IT *repository* che mantengono l'anagrafica del parco applicativo;
- risultati di investigazione degli strumenti di *discovery*;
- *blueprint* applicative ed eventuale ulteriore documentazione a supporto;
- interviste con i responsabili dei diversi applicativi qualora le sorgenti sopra citate non fossero sufficienti *all'assessment* di seguito descritto.

#### *1.20.1.1 Cloud readiness*

Per ***cloud readiness*** dell'applicativo si intende un modello di classificazione degli applicativi in relazione alla loro predisposizione alla migrazione in *cloud*. In prima istanza, vengono valutate le caratteristiche tecniche dell'applicativo secondo il seguente flusso logico:

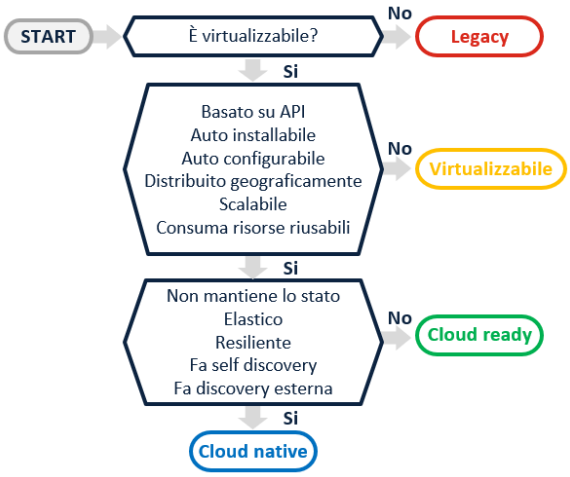



*Figura 40: Flusso logico di valutazione dell'applicativo*

In particolare:

- si definiscono "***legacy***" gli applicativi che non utilizzano ***hardware*** **comune**, ma richiedono *hardware* dedicato e non supportano tecnologie di virtualizzazione; l'**utilizzo di API** è assente e le attività di **installazione e *deployment*** sono in gran parte manuali. In presenza di architettura e configurazioni appropriate, si può garantire ***high availability***, ovvero permettere la ripresa anche solo parziale dell'operatività in una *Availability Zone* differente;
- si definiscono "**virtualizzabili**" gli applicativi che condividono *l'hardware* sottostante; come per i *legacy*, l'utilizzo di API è assente e le attività di installazione e *deployment* sono in gran parte manuali. In presenza di architettura e configurazioni appropriate, si può garantire *high availability*;
- si definiscono "***cloud ready***" gli applicativi che condividono *l'hardware* sottostante e per cui l'utilizzo di API è basato su logica esterna quale *scripting*. Le attività di installazione e *deployment* vengono automatizzate e tali applicativi possono essere **geo-distribuiti**, ovvero possono permettere la ripresa anche solo parziale dell'operatività in una *Availability Zone* di una differente Regione. Inoltre, sono in grado di **scalare orizzontalmente** per aumentare o diminuire la capacità in uso a seconda del carico di lavoro. Possono, altresì, **consumare risorse e servizi esterni** alla piattaforma su cui gira l'applicativo;
- si definiscono "***cloud native***" gli applicativi che condividono *l'hardware* sottostante e per cui l'utilizzo di API rappresenta il meccanismo di comunicazione *standard*. Le attività di installazione e *deployment* sono automatizzate, tali applicativi scalano orizzontalmente e sono geo-distribuiti. Consumano risorse e servizi esterni alla piattaforma su cui gira l'applicativo e soddisfano le seguenti ulteriori caratteristiche:
  - **l'assenza di informazioni** di stato e/o sessione;
  - **l'elasticità** (ovvero la gestione automatica dei cambiamenti in termini di utilizzo del servizio);
  - la **resilienza** (ovvero la capacità dell'applicativo di identificare e gestire automaticamente il ripristino della capacità e del servizio);
  - la capacità di fare ***discovery*** **di nuovi nodi** e risorse computazionali così come di servizi esterni alla piattaforma su cui gira l'applicativo.

#### *1.20.1.2 Requisiti funzionali e tecnici*

Il parco applicativo viene, quindi, analizzato rispetto a requisiti funzionali e tecnici quali:

- **confidenzialità del dato**: l'applicazione gestisce o meno informazioni sensibili (e.g. dati personali coperti da regolamentazioni locali quali GDPR);

- **architettura di alto livello**: principali componenti applicativi e modalità di interazione (e.g. architettura *multi-tier* che separa i componenti applicativi su diversi *layer* logici, architettura ad eventi dove la logica dell'applicativo è basata su funzioni di stato);
- **flessibilità del carico di lavoro**, carichi medi e picchi: un'applicazione può avere un carico più o meno prevedibile in termini di richiesta ed utilizzo delle risorse;
- **aspetti economico finanziari**: la natura dei costi può dipendere da una strategia di *sourcing* che richieda costi fissi, con possibilità di ammortamento, invece di costi che variano in base all'utilizzo.

#### *1.20.1.3 Piattaforma e sistema operativo sottostante l'applicativo*

La NewCo analizzerà ulteriormente gli applicativi al fine di mappare la piattaforma ed il sistema operativo attuali, distinguendo fra l'uso di *hardware* fisico o virtualizzato e verificando le eventuali dipendenze con il sistema operativo sottostante.

#### *1.20.1.4 Presenza di dipendenze*

La NewCo valuterà il caso in cui le singole applicazioni siano installate prevalentemente su architetture tecniche dedicate (silos) e verificherà **eventuali dipendenze ed interazioni** tra i diversi applicativi e le loro componenti. L'analisi richiede la disponibilità della documentazione e delle *blueprint* applicative e, qualora non sufficienti, l'utilizzo di strumenti e soluzioni *ad hoc* per ricostruire la mappa applicativa. Le interazioni tra applicativi verranno mappate sulle seguenti categorie:

- chiamate su *database* condiviso;
- chiamate tramite API;
- collegamento tramite *Message Bus*.

### 1.20.2 Analisi infrastrutturale

Al fine di consolidare e mappare la **situazione infrastrutturale** in essere, la NewCo utilizzerà le seguenti fonti di informazioni principali:

- il *Configuration Management Data Base* (CMDB), o eventuali altri IT *repository* che mantengono una vista sulle infrastrutture e le diverse piattaforme in uso;
- interviste con i responsabili dei sistemi e delle piattaforme qualora le sorgenti sopra citate non fossero sufficienti *all'assessment* di seguito descritto.

La NewCo studierà e ricostruirà, quindi, la situazione della PA utente in termini di:

- numero dei ***Data Center***, strategia di gestione (i.e. *in-house, outsourcing, co-location*), locazione e distanza, tipo di connettività e *tiering*;
- numerosità e tipologia dei ***server***, tecnologia e fornitore correnti, livello di *service continuity* supportato;
- dimensionamento e tipologia di ***storage***, tecnologia e fornitore correnti, *policy* di gestione dei dati in vigore;
- reale utilizzo dei **servizi applicativi ospitati**, inclusa la presenza di possibili ed effettivi sostituti;
- **obsolescenza infrastrutturale** e stato del supporto del fornitore;
- versione del **sistema operativo** e stato del supporto del fornitore;
- percentuale di **utilizzo** media e di picco, eventuale disponibilità di componenti di ricambio;
- tecnologia di **virtualizzazione** in uso;
- **architettura** *hardware*, inclusi bot di automazione e disponibilità di API.

La valutazione dell'infrastruttura viene svolta secondo il seguente flusso logico:

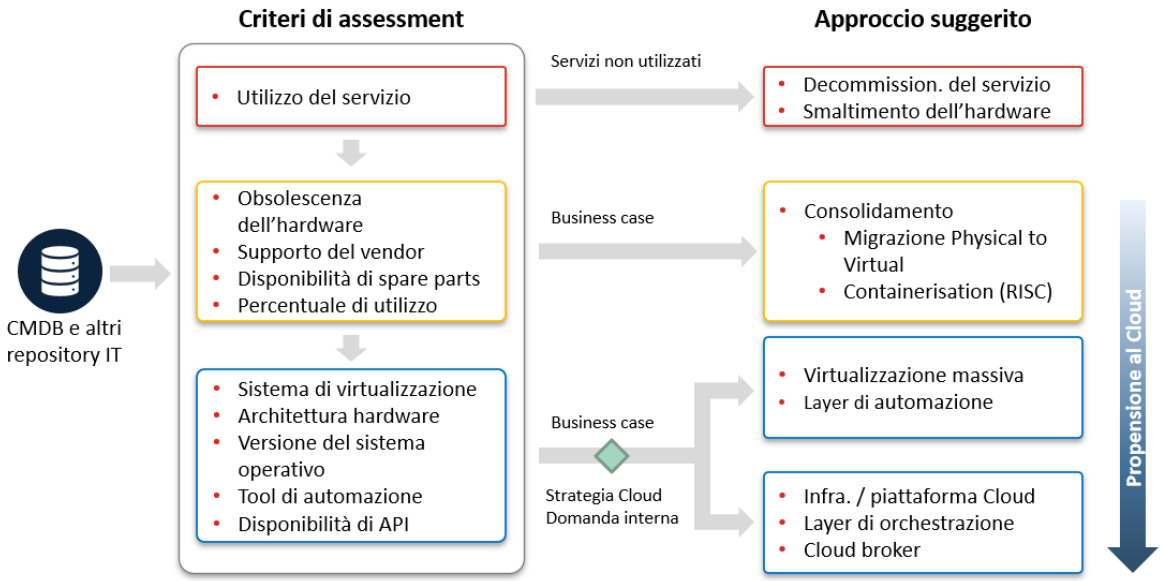



*Figura 41: Flusso logico di valutazione infrastrutturale*

### 1.20.3 Scenari di migrazione

La definizione delle azioni di intervento e relative *roadmap* parte dalla revisione dei principali esiti delle attività preliminari di valutazione applicativo-infrastrutturale:

- la *cloud readiness* dell'applicativo;
- i requisiti funzionali e tecnici dell'applicativo;
- la piattaforma e l'infrastruttura sottostanti e gli impatti derivanti dal reale utilizzo dei servizi applicativi, dall'obsolescenza infrastrutturale, dalla versione del sistema operativo e dallo stato del supporto da parte del fornitore.

L'Offerente propone di utilizzare il modello delle 6R (vedi Figura 42: Scenari di migrazione: modello delle 6R) al fine di categorizzare le principali azioni di intervento e definire le possibili strategie di trasformazione:

| | Remain (Housing) | Rehost | Replatform | Refactor | Revise | Rearchitect |
|---|---|---|---|---|---|---|
| Descrizione | Spostamento dell'infrastruttura fisica dagli attuali DC della PA ai DC del PSN/NewCo | Migrazione dell'applicativo AS-IS in ambiente Cloud con infrastruttura simile (Lift&Shift) | Migrazione sul Cloud con variazioni minime che consentono l'uso di piattaforme cloud-native | Migrazione dell'applicativo in Cloud con compatibilità retroattiva con i sistemi on-premise | Modifica del codice per modernizzare gli ambienti legacy introducendo logiche di virtualizzazione e automazione | Completa revisione dell'applicativo, trasformandolo in cloud-native |
| Benefici | • Non si effettua alcuna trasformazione, solo spostamento fisico | • Soluzione più semplice e veloce<br>• Import delle configurazioni AS-IS | • Facile implementazione<br>• Benefici cloud-native immediati | • Riutilizzo di framework applicativi e tecnologie container già utilizzate | • Soluzione propedeutica al refactor o rehost | • Riduzione dei costi nel lungo periodo<br>• Maggiore resilienza<br>• Operations semplificate |
| Rischi | • Presenza di servizi su sistemi in EOS<br>• Alti costi di gestione<br>• Difficoltà di gestione di sistemi legacy e difficilmente conformi agli standard (es. SOC) | • Cloud consumption inefficiente<br>• Problemi di scalabilità | • Cloud skill insufficienti<br>• Implementazione di cambiamenti drastici<br>• Operations massive in caso di mancanza di automazione | • Framework lock-in | • Spese elevate<br>• Time consuming | • Rischio di lock-in sul vendor<br>• Spese elevate<br>• Time consuming |

*Figura 42: Scenari di migrazione: modello delle 6R*

Tenendo presente che la strategia di trasformazione dei sistemi della PA prevede, in prima istanza, l'esclusivo utilizzo dei modelli di *Housing* e *Rehost* e solo nel medio e lungo termine i modelli di *Replatform* e *Rearchitect*, si riportano le valutazioni che l'Offerente intende fare per l'adozione del corretto modello, sottoforma di casi d'uso.
Gli applicativi classificati come "*legacy*" o "*virtualizzabili*" che hanno vincoli tecnici in termini di possibilità di migrazione e propensione al *cloud*, verranno considerati per le seguenti strategie di trasformazione ed azioni di intervento:

- dismissione, qualora il servizio non sia in uso o esistano sostituti (fruizione tramite SaaS);
- *housing* con servizio opzionale di *moving* fisico;
- migrazione da fisico a virtuale (*Rehost*) qualora il sistema sia compatibile con tecnologie di virtualizzazione quali *hypervisor*;
- migrazione da virtuale a virtuale (*Rehost*) con eventuale possibilità di ridimensionamento infrastrutturale al fine di ottimizzare l'utilizzo della capacità in proporzione alle *performance* ed ai livelli di servizio richiesti.




*Figura 43: Caso di consolidamento*

Gli applicativi classificati come "*virtualizzabili*" che non presentano vincoli tecnici in termini di possibilità di migrazione e propensione al *cloud*, verranno considerati per le seguenti strategie di trasformazione ed azioni di intervento:

- migrazione su *cloud* tramite configurazioni minori quali:
  - la creazione di *script* per abilitare l'automazione di determinati *task*;
  - l'utilizzo di soluzioni di automazione quali *bot* e *container*.




*Figura 44: Casi di applicativo virtualizzabile*

Gli applicativi classificati come "*cloud ready*" e "*cloud native*", ovvero da considerarsi propensi all'adozione del *cloud*, verranno considerati per le seguenti strategie di trasformazione ed azioni di intervento:

- migrazione as-is su un unico ambiente *cloud*;
- alternativamente, ed in caso di particolari requisiti quali la confidenzialità e sensibilità dei dati, revisione architetturale per permettere la migrazione in *Private Cloud* delle componenti applicative che ospitano ed eseguono transazioni su dati sensibili ed in *Public Cloud* delle componenti applicative che beneficiano maggiormente della scalabilità e del portafoglio di servizi offerti dai fornitori di *Public Cloud*.

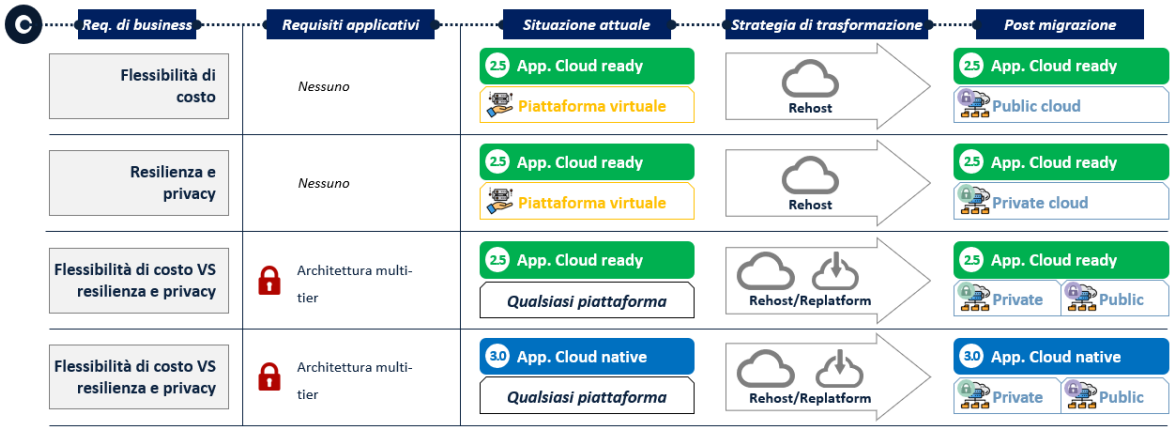



*Figura 45: Casi di applicativo cloud Ready e cloud Native*

Nell'ottica di un processo di consolidamento dei sistemi della PA utenti, la NewCo prenderà in considerazione anche la dismissione di un applicativo e relativa infrastruttura per rimpiazzarlo con una soluzione SaaS con le stesse (o simili) funzionalità.
In particolare, la trasformazione di un applicativo in *cloud* tramite l'acquisizione di un pacchetto applicativo SaaS comporta una serie di benefici rispetto all'utilizzo di soluzioni *on-premises*:

- non è richiesta infrastruttura e la potenza computazionale necessaria è trasparente all'utente;
- si riduce la forza lavoro necessaria alle attività di operatività e manutenzione dell'applicativo;
- il modello di costo è trasparente e caratterizzato da frequenti rendicontazioni;
- l'installazione è molto più rapida grazie ad una minima necessità di configurazione, limitata alla configurazione degli utenti e dei relativi accessi;
- vi è disponibilità di aggiornamenti costanti che non impattano il servizio.




*Figura 46: Caso SaaS*

Contestualmente a questa attività di *assessment*, le aree di intervento vengono identificate come critiche e prioritizzate in base a tre *driver* principali:

- non conformità rispetto alle linee guida sulla sicurezza o alle regolamentazioni esterne;
- ottimizzazione dei costi tramite revisione dell'infrastruttura oppure adozione di un modello SaaS, quest'ultimo da valutarsi tramite un *business case* dedicato;
- automazione di attività ricorsive manuali.

Tutti i modelli di trasformazione sopracitati potrebbero essere intrapresi sin da subito, come soluzioni *target*; tuttavia, la NewCo si atterrà ai *desiderata* della PA utenti e proseguirà con una strategia incrementale:

1. nel breve termine, tutti i sistemi verranno migrati con approccio di *Rehost* su nuove piattaforme o tramite *housing/hosting* della piattaforma esistente;
2. nel medio termine, si utilizzano gli approcci di *Replatform* e *Revise*, che consentono di sfruttare logiche di automazione e ottimizzazione della capacità delle risorse; considerando sistemi che in prima istanza sono soggetti a semplice *Housing*, l'approccio di *Rehost* può essere inteso come un'evoluzione di medio termine;

3 **nel lungo termine**, si utilizzano gli approcci di *Refactor* e *Rearchitect*, procedendo con la modifica parziale o totale dell'applicativo che favorisca l'adozione di logiche *cloud native*.

La figura seguente riporta questa strategia incrementale, mappando gli approcci lungo la linea temporale ed evidenziandone l'ingenza dei costi:

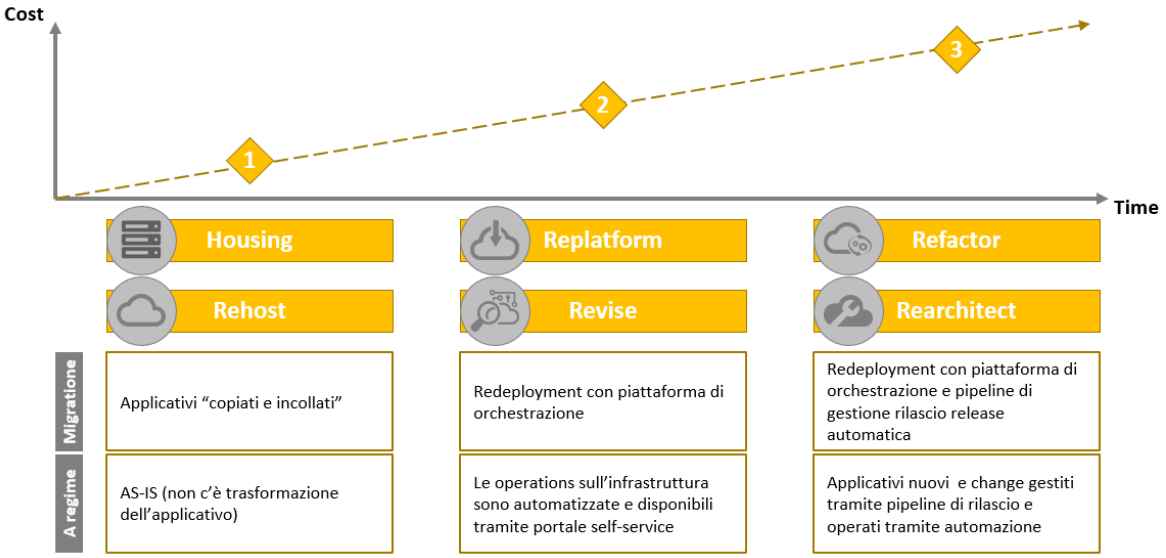



*Figura 47: Scenari di migrazione per la PA*

A seconda del grado di trasformazione selezionato e della dimensione della PA utente, si identificano tre livelli di complessità: bassa, media, alta. Si esporta la seguente convenzione, a titolo esemplificativo, per la classificazione della dimensione della PA utente:

- PA di piccola dimensione: fino a 10 *rack*;
- PA di media dimensione: fino a 20 *rack*;
- PA di grande dimensione: oltre 20 *rack*.

*Tabella 12: Scenari di complessità della migrazione*

| | PA di piccola dimensione | PA di media dimensione | PA di grande dimensione |
|---|---|---|---|
| Housing/Rehost | Bassa | Media | Media |
| Replatform/Revise | Media | Alta | Alta |
| Refactor/ Rearchitect | Media | Alta | Alta |

Il livello di complessità dello scenario di migrazione incide sul *team mix* necessario allo svolgimento delle attività: ogni tipologia di trasformazione richiede profili con specifiche caratteristiche tecniche; la dimensione della PA incide sulla numerosità delle risorse necessarie.
Si riporta, a titolo esemplificativo, una proposta per le tempistiche previste per il piano di migrazione:

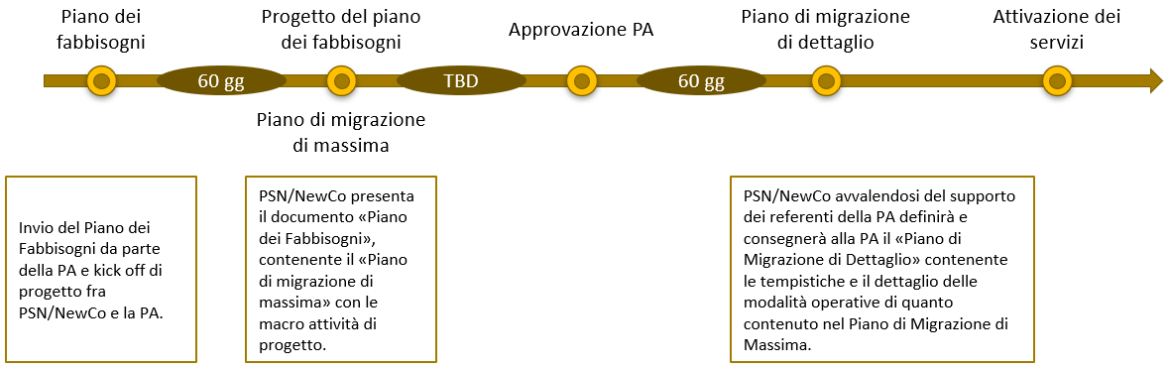



*Figura 48: Piano di migrazione (esemplificativo)*

A seconda dello scenario di complessità, si declina il Piano di Migrazione:

- **scenario ad alta complessità**: il "*Piano di Migrazione di Dettaglio*" dovrà evidenziare gli aspetti logistici, infrastrutturali, organizzativi e procedurali previsti per l'erogazione di quanto contenuto nel "*Piano di Migrazione di Massima*", nonché la pianificazione temporale con cui verranno effettuate le attività;
- **scenario a media complessità**: il piano contiene anche le proposte evolutive nel medio termine;
- **scenario a bassa complessità**: il piano contiene anche le proposte evolutive nel medio e lungo termine.

Come illustrato nell'Offerta, sebbene sia possibile ottimizzare la pianificazione, mediante *team mix ad-hoc* e categorizzazione di dettaglio della singola migrazione, la pianificazione complessiva del singolo progetto dipende anche da fattori non direttamente controllabili dal personale della NewCo, quali: *committment* degli *stakeholder*, disponibilità di documentazione, livello di customizzazione della singola applicazione, etc.
Alla luce di quanto detto, il piano di dettaglio dovrà necessariamente tener conto delle specificità di ogni singola migrazione.

### 1.20.4 Figure Professionali e Team mix per gli scenari di migrazione

La NewCo renderà disponibili risorse professionali proprie o di *partner*, quali HPE, VMWare o altri, che hanno all'attivo il successo di importanti programmi di migrazione, svolti per la Pubblica Amministrazione. Tali figure supporteranno le PA utenti in tutte le attività/necessità che emergeranno nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (*rehost, rearchitect, replatform*), proseguendo nella fase di riavvio degli applicativi, *regression test* e terminando nel supporto all'esercizio.
Per ogni progetto, verrà individuato il *mix* di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo, che effettuerà le attività richieste. Il *team mix* potrà essere composto da una o più delle seguenti figure professionali:

- ***Project Manager***: definisce e gestisce i progetti, adottando e promuovendo metodologie agili; è responsabile del raggiungimento dei risultati, conformi agli standard di qualità, sicurezza e sostenibilità, in coerenza con gli obiettivi, le performance, i costi ed i tempi definiti;
- ***Enterprise Architect***: ha elevate conoscenze su differenti aree tecnologiche che gli permettono di progettare architetture *enterprise*, sviluppando modelli basati su *Enterprise Framework*; è responsabile di definire la strategia abilitante per l'evoluzione

dell'architettura, mettendo in relazione la missione di *business*, i processi e l'infrastruttura necessaria;

- *Cloud Application Architect*: ha conoscenze approfondite ed esperienze progettuali nella definizione di architetture complesse e di Ingegneria del *Software* dei sistemi *cloud* ed agisce come *team leader* degli sviluppatori ed esperti tecnici; è responsabile della progettazione dell'architettura di soluzioni applicative di *cloud computing*, assicurando che le procedure ed i modelli di sviluppo siano aggiornati e conformi agli *standard* ed alle linee guida applicabili;
- *Cloud Application Specialist*: ha consolidate conoscenze tecnologiche delle soluzioni *cloud* e dell'integrazione di soluzioni applicative basate su un approccio *cloud computing based*; è responsabile della *delivery* di progetti basati su soluzioni *cloud*;
- *Business Analyst*: è responsabile dell'analisi dei dati anche in ottica di *business*, e della relativa raccolta dei requisiti necessari a migliorare la qualità complessiva dei servizi IT forniti;
- *Cloud Security Specialist*: esperto nella progettazione di architetture di sicurezza per sistemi basati su *cloud* (*public* ed *hybrid*). È responsabile per il supporto alla realizzazione delle architetture di sicurezza dei nuovi *workload* delle Amministrazioni utenti ed alle attività di migrazione, fornisce indicazioni e raccomandazioni strategiche ai gruppi operativi e di sviluppo per affrontare i punti deboli della sicurezza ed identificare potenziali nuove soluzioni di sicurezza negli ambienti *cloud*;
- *Database Specialist and Administrator*: è responsabile dell'installazione, dell'aggiornamento, della migrazione e della manutenzione del DBMS; si occupa di strutturare e regolamentare l'accesso ai DB, monitorarne l'utilizzo, ottimizzarne le prestazioni e progettare strategie di *backup*;
- *Middleware Specialist*: definisce, sviluppa e supporta soluzioni di *Enterprise Application Integration* (EAI) che includono integrazione applicativa, gestione API e *streaming*;
- *DevOps Expert*: Ha consolidata esperienza nelle metodologie di sviluppo DevOps su progetti complessi, per applicare un approccio interfunzionale in grado di garantire la sinergia tra i gruppi di sviluppo e di gestione dei sistemi; è responsabile di progettare le strategie DevOps, identificando gli strumenti di controllo dei sorgenti, di automazione e di rilascio in ottica *Continuous Integration* e *Continuous Development*;
- *System and Network Administrator*: ha competenze sui sistemi operativi, *framework* di containerizzazione, tecnologie di virtualizzazione, orchestratori e sistemi di *configuration* e *versioning*; è responsabile dell'implementazione di sistemi di virtualizzazione, di *container*, utilizzando anche sistemi di orchestrazione e della manutenzione, della configurazione e del funzionamento dei sistemi informatici di base;
- *Developer (Cloud/Mobile/Front-End Developer)*: ha competenze di linguaggi di programmazione e di piattaforme di sviluppo, utilizza le metodologie di analisi e disegno OOA, SOA e REST con UML; assicura la realizzazione e l'implementazione di applicazioni con architetture *web-based* e *cloud-based*;
- *UX Designer*: ha una conoscenza teorica e pratica dei principi di usabilità, paradigmi di interazione e principi di i*nteraction design* e di gestione delle problematiche di compatibilità *cross-browser* (*desktop, tablet, mobile*); è responsabile dell'applicazione dell'approccio centrato sull'utente (*human centered*) nello sviluppo dei servizi digitali, garantendo il raggiungimento efficace ed efficiente degli obiettivi dell'utente nell'interazione con l'Amministrazione;
- *System Architect*: ha consolidata esperienza in *technical/service management* e *project management*, analizza i sistemi esistenti e definisce come devono essere coerentemente integrate le nuove soluzioni; è responsabile della progettazione della soluzione infrastrutturale e del coordinamento di specifici stream di progetto;

- *Product/Network/Technical Specialist*: è responsabile delle attività inerenti all'integrazione delle soluzioni tecniche ed il supporto specialistico di prodotto nell'ambito dell'intervento progettuale;
- *Security Principal*: definisce, implementa e gestisce gli aspetti di sicurezza dei progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli *standard* di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le *performance*, i costi ed i tempi definiti;
- *Senior Information Security Consultant*: presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, un sito) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di *governance* della *cyber security* ed il resto del personale operativo. Controlla il rispetto delle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti ed i sistemi informatici di un'organizzazione;
- *Information Security Consultant*: garantisce l'esecuzione delle misure di sicurezza per proteggere le reti ed i sistemi informatici. Attua le regole definite in materia di sicurezza delle informazioni;
- *Senior Security Auditor/Analyst*: garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Gestisce l'esame periodico della sicurezza di sistemi, reti ed applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto alle regole interne, normative esterne e *best practice* internazionali in materia. Completa i giornali di *audit* documentando *test* e risultati dell'*audit*;
- *Security Solution Architect*: progetta, costruisce, esegue *test* ed implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico;
- *Data Protection Specialist*: figura professionale dedicata ad affiancare il titolare, gli addetti ed i responsabili del trattamento dei dati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo GDPR;
- *Junior Security Analyst*: gestisce l'esame periodico della sicurezza di sistemi, reti ed applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto alle regole interne, normative esterne e *best practice* internazionali in materia;
- *Machine Learning Engineer/Data Scientist*: si occupa della progettazione e sviluppo di algoritmi di apprendimento automatico, della preparazione ed analisi di dati storici per identificare i *pattern*, dello sviluppo di nuovi metodi analitici laddove quelli adottati risultino obsoleti e dell'esecuzione di analisi esplicative dei dati; si occupa di monitorare e curare il flusso di dati, gli algoritmi ed interviene prontamente in caso di cali di *performance*;
- *Artificial Intelligence Specialist*: si occupa di implementare e gestire le principali tecnologie e piattaforme che utilizzano l'intelligenza artificiale, quali creazione di servizi di IoT e *chatbot*, dell'automazione delle attività di routine, dell'elaborazione di grandi data set e dell'implementazione di sistemi di *Image Analysis* per la sicurezza dell'infrastruttura;
- *Big Data Architect*: comprende la varietà dei dati trattati (strutturati, semi strutturati e destrutturati) e li analizza per definire modelli e sistemi mirati a gestirne l'eterogeneità, tenendo conto del volume di dati, del flusso (includendo anche stream processing) e della durabilità;
- *Forensic Expert*: è chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale;

- *Senior Penetration Tester*: definito anche *ethical hacker*, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio;
- *Junior Penetration Tester*: effettua tentativi di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza in accordo con quanto definito nel progetto di riferimento;
- *System Integration & Test Specialist*: contribuisce in differenti aree dello sviluppo del sistema, effettuando il *testing* delle funzionalità, identificando le anomalie e diagnosticandone le possibili cause. Utilizza e promuove strumenti automatici;
- *Educational Designer/Tutoring*: struttura, organizza e schedula i programmi di formazione, ne valuta la qualità attraverso un processo di *feedback*.

Per supportare la fase di migrazione, la NewCo metterà a disposizione le seguenti figure professionali:

- *Project Manager*: coordina le attività e collabora con il referente che ogni singola PA utente dovrà indicare e mettere a disposizione;
- *Technical Team Leader*: segue, guida e monitora tutte le fasi concernenti gli aspetti tecnici e operativi.

A seconda del modello di trasformazione intrapreso, saranno forniti a titolo esemplificativo i seguenti *team mix*:

- *Housing / Hosting / Rehost*: figure specializzate sugli aspetti infrastrutturali, in grado di gestire migrazioni fisiche e logiche;
- *Replatform / Revise / Refactor / Rearchitect*: aggiunta di figure specializzate in ambito applicativo, che possano studiare la situazione attuale ed eventualmente procedere alla modifica massiva del codice.

*Tabella 13: Team mix per scenari di migrazione*

| Housing/Hosting/Rehost | Replatform/Revise/Refactor/Rearchitect |
|---|---|
| • *Enterprise Architect*<br>• *System Architect*<br>• *Cloud Application Architect*<br>• *Cloud Application Specialist* | • *Enterprise Architect*<br>• *System Architect*<br>• *Cloud Application Architect*<br>• *Cloud Application Specialist*<br>• *Developer*<br>• *UX Designer*<br>• *System and Network Administrator*<br>• *DevOps Expert* |

La dimensione della PA inciderà sul *team mix* in termini di numerosità dei profili forniti.

## 1.21 ID CRITERIO:21 – VALUTATIVO - MIGLIORAMENTI DEL MODELLO ORGANIZZATIVO, DELLE METODOLOGIE E DEGLI STRUMENTI CHE IL CONCORRENTE SI IMPEGNA AD ADOTTARE PER IL MONITORAGGIO ED IL CONTROLLO DELLA MIGRAZIONE AL FINE DEL RISPETTO DELLE TEMPISTICHE PREVISTE.

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 21 | Valutazione | Migrazione | Miglioramento delle modalità per la migrazione in *cloud* - Monitoraggio e gestione della migrazione | Miglioramenti del modello organizzativo, delle metodologie e degli strumenti che il concorrente si impegna ad adottare per il monitoraggio ed il controllo della migrazione al fine del rispetto delle tempistiche previste. | **3** |

Questa sezione descrive i miglioramenti del modello organizzativo, delle metodologie e degli strumenti che l'Offerente propone per il monitoraggio ed il controllo della migrazione, come da descrizione del criterio valutativo 21.
Come indicato nel criterio 20, anche in questo caso, a beneficio della **trasparenza e verificabilità** dei miglioramenti descritti in questa sezione, l'Offerente, impegnandosi ad utilizzare degli **strumenti per il monitoraggio ed il controllo delle migrazioni**, propone di:

- **rendere oggetto di possibili *audit* da parte del Concedente** (ove possibile, ad es. *tool* proprietari), per verificarne l'effettiva affidabilità;
- **rendere accessibili al Concedente** (ove possibile), per monitorare costantemente l'andamento complessivo delle migrazioni.

### 1.21.1 Gestione di progetto (*project management*)

Per gestire la fase di migrazione dei servizi della PA utente sul PSN, l'Offerente propone l'implementazione di un Modello Operativo in cui spiccano due funzioni di cruciale importanza per garantire lo svolgimento progettuale e2e (*end to end*) nei tempi, nelle modalità e nei costi concordati con la PA utente.

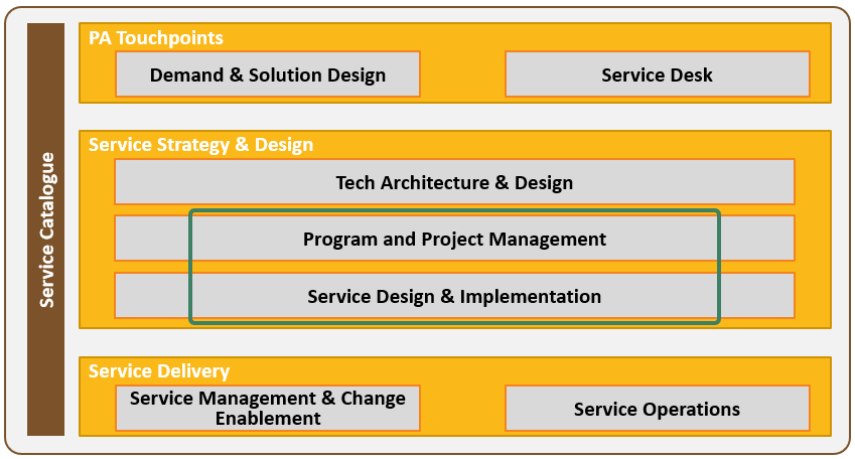



*Figura 49: Modello Operativo ad alto livello*

- funzione di ***Program and Project Management***: si occupa di *governance* progettuale relativa alla migrazione dei servizi della PA utente; le principali attività sono:
  - definizione degli *stakeholder* e della matrice RACI tra la PA utente e la NewCo o gli *Hyperscaler*;
  - identificazione delle risorse della NewCo, appartenenti alla funzione di *Service Design & Implementation* per l'esecuzione delle attività;
  - estrapolazione delle assunzioni alla base delle soluzioni, a partire dal disegno architetturale;
  - definizione del piano di lavoro e condivisione con la PA utente e successiva gestione delle attività nel tempo;
  - monitoraggio dello stato di avanzamento delle attività e condivisione con la PA;
  - gestione dei rischi e dei problemi;
  - gestione del processo di produzione e condivisione dei *deliverable*.

- funzione di ***Service Design and Implementation***: si occupa della vera e propria migrazione dei servizi della PA utente, conducendo principalmente le seguenti attività:
    - affinamento del disegno di dettaglio della soluzione nel caso di variazioni infrastrutturali o validazione del disegno esistente, in linea con quanto definito e condiviso dalla PA utente nella fase di Disegno;
    - svolgimento di tutte le attività di implementazione del nuovo servizio, fino al rilascio in produzione;
    - interfacciamento con la funzione di *Program & Project Management* durante l'esecuzione delle attività progettuali per condividere lo stato avanzamento lavori, sottolineare criticità o problematiche o dipendenze emerse;
    - *knowledge Transfer* verso le strutture di *Service Delivery*.

### 1.21.2 Comunicazione avanzamento di progetto

Per mantenere una comunicazione **trasparente** ed il ***focus* sugli obiettivi di progetto** (strategico, tattico e operativo), l'Offerente propone tre categorie di *meeting*, secondo il seguente schema:

*Tabella 14: Tipologie di meeting*

| Meeting | Partecipanti | Frequenza suggerita |
|---|---|---|
| Executive Steering Committee | • Rappresentanti di *Governance* del contratto fra la NewCo e la PA utente<br>• *Program Manager* della PA utente<br>• *Program Manager* della NewCo | Mensile |
| SAL | • *Program Manager* della PA utente<br>• *T&T Integration Manager* della NewCo<br>• *Delivery Project Executive* della NewCo<br>• Rappresentanti del *team* di progetto da definire secondo la necessità | Settimanale |
| Meeting per area/ sotto progetto | • PM della NewCo, referenti della PA utente per area/sotto progetto | Settimanale/ all'occorrenza |

I *meeting* di stato del progetto si focalizzeranno sulle seguenti aree:

- obiettivi raggiunti/attività concluse nel periodo precedente al *meeting*;
- attività pianificate nel periodo seguente;
- tracciamento di rischi e problemi e delle azioni mitigative/risolutive;
- stato delle *milestone*;
- stato dei *deliverable*;
- progresso del progetto;
- *project Change Request*.

È responsabilità del *Project Management* della NewCo la stesura del verbale di riunione, la raccolta delle approvazioni ed, infine, la distribuzione dello stesso agli *stakeholder* per comunicazione.
Di seguito, si riporta un esempio di *Dashboard* di progetto, a scopo illustrativo:

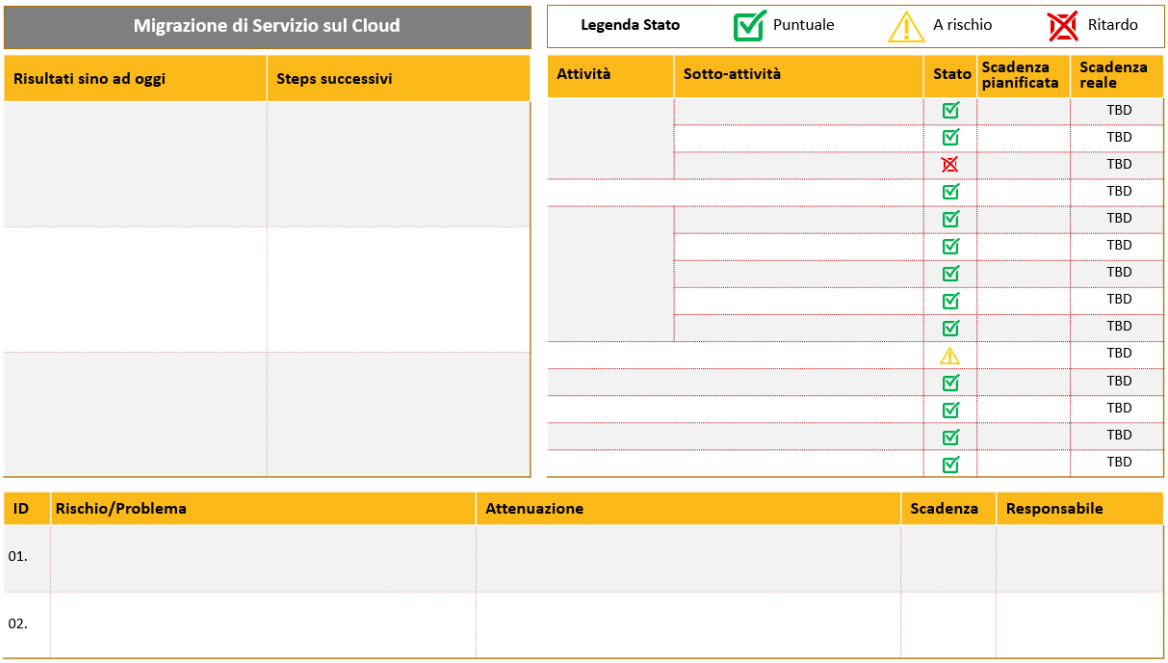



*Figura 50: Dashboard di progetto (illustrativa)*

### *1.21.3 Service management*

La funzione di *Service Management* della NewCo è responsabile dell'erogazione dei servizi ospitati in modalità *hosting/housing* e *Private Cloud* in linea con i livelli di servizio concordati, che sono monitorati mediante l'utilizzo di *tool* automatici di SLA *Management* e di strumenti di *reporting*.

In funzione della tipologia dei livelli di servizio da implementare, l'Offerente prevede di rilevare ed aggregare dati elementari afferenti a diversi processi, quali *Request Fulfilment*, *Incident*, *Problem*, *Change*, *Availability* e *Performance Management*, e provenienti da diversi strumenti.

La figura del *Service Manager* ha il ruolo primario di interfacciamento con la PA utente, per tutti gli aspetti relativi all'erogazione del servizio previsto nel Contratto ed alla gestione dei rapporti e delle relazioni tecniche e operative.

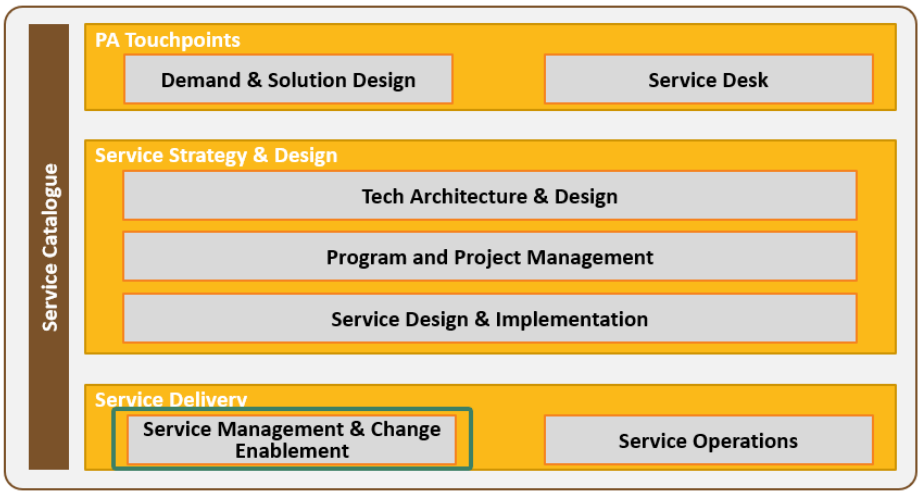



*Figura 51: Modello Operativo ad alto livello: funzione di Service Management*

Al *Service Manager* riportano funzionalmente tutti i *Tower Lead* della funzione di *Service Operation*. Le responsabilità del *Service Manager* sono:

- interfacciarsi costantemente e collaborare con i referenti dell'IT della PA utente;

- monitorare in modo continuativo e sistematico i livelli di servizio, i KPI, la puntualità e la qualità del servizio erogato dalle strutture tecniche della NewCo e da eventuali fornitori esterni, verificandone la coerenza con quanto indicato e definito nel contratto in un'ottica di continuo miglioramento;
- predisporre i *report* sullo stato del servizio e sulle azioni pianificate per mantenere e migliorare lo stesso;
- impostare le modalità di rilevazione e consuntivazione degli eventuali servizi aggiuntivi e predisporre mensilmente i report dei consuntivi;
- essere parte attiva adoperandosi ai fini della risoluzione di conflitti o problemi o dispute che dovessero insorgere nel corso del contratto;
- gestire raccolta, estrazione, consolidamento, analisi, comunicazione e condivisione dati.

Inoltre, il *Service Manager* deve organizzare incontri mensili di verifica formale dell'andamento dell'erogazione dei servizi rispetto a quanto stabilito a contratto.
In questi incontri di *Operation Review*:

- si analizzano i *report* sulle *performance* di ciascun servizio, verificandone gli SLA ed i KPI, e si controllano eventuali deviazioni rispetto a quanto condiviso contrattualmente;
- vengono esaminati eventuali incidenti critici occorsi. Nel caso ci fossero degli incidenti ancora irrisolti, si potrà attivare la procedura di *escalation*.

Il *Service Manager* provvede, in seguito al meeting di *Operation Review*, a redigere un verbale dove si riportano:

- le proposte per la risoluzione degli incidenti critici;
- le ragioni degli eventuali scostamenti rispetto agli SLA;
- piani di dettaglio di interventi, qualora fossero necessari.

### 1.21.4 *Change enablement* a supporto della migrazione

Come illustrato nella *Figura 51: Modello Operativo ad alto livello: funzione di Service Management*, all'interno della funzione di *Service Management* si trova il *layer* di IT ***Change Enablement***, composto da esperti di *Change Management*, *Project Management*, *Architetture*. Quest'ultimo si interfaccia con la PA utente e la funzione di *Service Operations* della NewCo, per lo svolgimento delle seguenti attività:

- mantenere i rapporti con le diverse entità PA impattate dalla migrazione;
- pianificare e gestire le migrazioni;
- interfacciarsi con il dipartimento IT / *team* di *Operations* della NewCo;
- interfacciarsi con il *Service Manager* per la valutazione e minimizzazione degli impatti della migrazione sugli SLA;
- interfacciarsi con i *vendor* tecnologici.

Le attività in carico al *Change Enablement* assicurano che tutti gli oggetti di tracciamento (CRQ) siano nel corretto stato (e.g. in *progress*, in *implementation*, *completed*), che gli *stakeholder* impattati siano informati e che il programma di implementazione sia coordinato con tutte le altre attività dell'organizzazione, garantendo alla PA utente un alto livello di disponibilità e servizio.
Le migrazioni vengono pianificate ed implementate attraverso *wave* e tracciate tramite opportuni processi e strumenti di *ticketing*; per il controllo e la limitazione degli impatti, si favoriscono le migrazioni logiche e virtuali (*Physical* to *Virtual* e *Virtual to Virtual*) e si propone l'utilizzo di un prodotto basato su tecnologie *Open Source* per il **controllo dei *clash*** tra le attività.

#### *1.21.4.1 Operatività del layer di Service Management*

Operativamente, il *layer* di *Change Enablement* si occupa di:

- pianificare le migrazioni di progetto: il *layer* di *Change Enablement* riceve lo *scope* di progetto dalla PA utente con vincoli e *deadline* associati. Grazie al supporto della documentazione tecnica raccolta, viene svolta un'attività di analisi per identificare la soluzione infrastrutturale *target*, individuare eventuali criticità e definire le *wave* di migrazione. Il piano di progetto viene condiviso con la PA utente per approvazione. Più nel dettaglio:
    - ricezione del piano dei fabbisogni con relative *deadline*, vincoli, HLD, *milestone*: la PA utente fornisce al *layer* di Change *Enablement* l'elenco dei sistemi e delle applicazioni in scope al progetto di migrazione (Piano Dei Fabbisogni). In questa fase, si definiscono le *deadline* da rispettare, eventuali vincoli in essere, le criticità su particolari sistemi/applicazioni, in modo da ottenere una visione complessiva del progetto.
    - analisi dei sistemi, applicazioni in scope ed individuazione criticità: sulla base del piano dei fabbisogni fornito dalla PA utente, viene avviata una fase di analisi dei singoli sistemi/applicazioni con l'obiettivo di definire una categorizzazione per piattaforma fisica o virtuale, sistema operativo, tecnologie, relazioni e dipendenze con altri sistemi, condivisione di DB/*repository*, utilizzo di specifici sistemi di autenticazione e *network* di appartenenza, etc.
    - raccolta/stesura documentazione tecnica: si raccoglie la documentazione relativa a sistemi ed applicazioni in *scope* in modo da ricostruire una conoscenza di base degli stessi. La documentazione dovrà essere fornita dalla PA utente (soprattutto nel caso di applicazioni proprietarie o architetture fuori *standard*). Nel caso questo non fosse possibile, si dovrà procedere a reperire queste informazioni tramite interviste con i *Service Owner*, gli specialisti di sistema, in *workshop* dedicati.
    - scelta del modello di trasformazione: sulla base dei tecnicismi raccolti e delle analisi effettuate, si procede ad identificare il modello di trasformazione da adottare nel processo di migrazione, scegliendo fra: *Housing*, *Rehost*, *Replatform*, *Revise*, *Refactor*, *Rearchitect*. Viene quindi ingaggiato il *team mix* corrispondente e si identificano i *tool* a supporto.
    - individuazione della granularità delle attività di migrazione: tramite il supporto dei *Service Owner*, si definiscono le *wave* di migrazione secondo parametri tecnici e di business, quali considerazioni di omogeneità della tipologia di ambiente (*Dev, Test, Prod*), dei servizi relazionati e dipendenti tra loro e l'eventuale approssimarsi dello stato di *End of Life* (EoL) dei sistemi in *scope*. In particolare, viene data priorità agli ambienti di non produzione per la loro bassa criticità ed ai sistemi che presentano problematiche operative che possono essere risolte con la migrazione.
    - creazione del piano di migrazione del progetto: una volta definite le *wave* di migrazione e scelte le soluzioni *target*, viene creato un primo piano di migrazione del progetto che terrà in considerazione le deadline da rispettare e gli eventuali vincoli forniti dalla PA utente, per tener conto di criticità particolari di sistemi ed applicazioni.
    - condivisione del piano di migrazione del progetto con la PA utente per approvazione: il piano di migrazione del progetto inclusivo delle *wave* precedentemente definite viene condiviso e discusso con i principali *stakeholder* al fine di verificarne l'affinità con le esigenze della PA utente ed ottenerne l'approvazione.
- tracciamento delle migrazioni attraverso *wave*: il tracciamento attraverso *wave* serve a supportare la pianificazione ed il monitoraggio dell'avanzamento delle migrazioni dei sistemi della PA utente all'interno dei DC della NewCo e degli *Hyperscaler*. Nel dettaglio, si svolgono le seguenti attività:

- creazione del piano di migrazione di ogni *wave*: i piani delle singole *wave* vengono dettagliati includendo tutti i sistemi impattati ed aggregandoli secondo specifici criteri di appartenenza, ottimizzando i tempi ed efficientando le risorse. Sulla base dei criteri forniti dalla PA utente, i sistemi vengono prioritizzati all'interno della *wave*, specificando le date di migrazione di ogni singolo sistema, all'interno del *timeframe* concordato con la PA utente;
- creazione del ticket per ogni *wave*: si crea l'oggetto contenitore nel sistema di *ticketing* che funge da aggregatore per la *wave* di tutte le migrazioni che verranno indirizzate tramite singole CRQ. Questo permette di tracciare e monitorare complessivamente l'andamento delle *wave*;
- definizione delle macro-attività e comunicazione ai *team* coinvolti: per ogni *wave*, si coinvolgono i *team* operativi per verificare e pianificare le attività preparatorie propedeutiche alle migrazioni, che consistono nella messa in sicurezza dei sistemi *target* ed aggiornamento all'ultimo livello di *patch* possibile per garantire piena compatibilità con l'ambiente *target*.
  Dal punto di vista di *networking*, e nel caso di migrazioni di particolare complessità, si implementano le configurazioni necessarie all'estensione delle *subnet* tramite soluzioni quali *spine connection*, *fabric path gateway*. Nel caso di migrazione fisica nei DC della NewCo (*housing*) gli specialisti di sistema ed i *Vendor* saranno preallertati allo scopo di garantire il loro intervento e per prevedere un magazzino disponibile per le parti *hardware* che potrebbero essere soggette a rottura durante la migrazione;
- tracciamento pianificazione ed avanzamento: per ogni *wave*, si dettaglia la vista sulle attività terminate con successo e di quelle che devono necessariamente essere ripianificate. Le analisi sugli esiti delle migrazioni, i problemi riscontrati e le relative soluzioni adottate, alimentano una base di conoscenza finalizzata a perfezionare progressivamente le migrazioni stesse;
- allineamento *stakeholder* impattati: gli *stakeholder* interessati vengono coinvolti in *meeting* settimanali di avanzamento lavori (SAL) in cui viene illustrato l'avanzamento di progetto e si discutono eventuali criticità emerse, quali la necessità da parte della PA utente di modificare la pianificazione relativa a determinate migrazioni, anticipandole o posticipandole per esigenze tecniche o di *business*. Puntuali comunicazioni vengono inoltre inviate per gestire tempestivamente specifiche criticità o emergenze;

- gestione operativa delle CRQ di migrazione: dopo aver creato le singole CRQ di migrazione relative alle *wave* identificate, il *layer* di *Change Enablement* supporta la funzione di *Operations* nella stesura del piano di migrazione analizzando eventuali impatti e disservizi. Usufruendo della piattaforma di controllo e tracciamento, si verificano eventuali *clash* e si individuano possibili consolidamenti. Dopo aver raccolto le approvazioni dei vari *Change Advisory Board* (CAB), si ingaggiano i *team* coinvolti e si procede con il coordinamento della migrazione, gestendo le attività preparatorie e post migrazione. Nel dettaglio:
  - creazione di un *ticket* per ogni migrazione: si crea una CRQ per la migrazione di ogni singolo *server*, *cluster* o applicativo. Tutti gli *asset* coinvolti nella migrazione vengono relazionati alla CRQ in modo da poter verificare eventuali *clash* con altre attività. Ogni CRQ è inoltre relazionata al *ticket* della *wave* di appartenenza;
  - stesura di un *Deployment Plan* e relativa pianificazione: per ogni migrazione viene creato congiuntamente ai *team* operativi un *Deployment Plan* ("DP"), in cui l'attività di migrazione viene esplosa in singoli *task* caratterizzati da data e ora di inizio e di fine, l'assegnatario del *task* ed eventuali gruppi a supporto. Il DP è strutturato in modo da prevedere *check point* di verifica dell'andamento dell'attività con differenti flussi operativi conseguenti all'esito dei *task* effettuati

(*Go/No Go*). In caso di esito positivo (*Go*) del *check point*, l'attività prosegue con le *task* successive fino alla conclusione della migrazione. In caso di esito negativo (*No Go*), vengono implementati le *task* necessarie alla procedura di ripristino dei sistemi (*rollback*);

- **analisi degli impatti e dei disservizi**: la lettura del *Deployment Plan* da parte dei sistemisti supporta l'analisi degli impatti dei disservizi e l'identificazione di eventuale presenza di ridondanza sui sistemi (*cluster*, bilanciatori), che può essere sfruttata per la definizione ed implementazione della procedura operativa più idonea a garantire la continuità del servizio;
- **consolidamento di *ticket* impattanti gli stessi sistemi**: con il supporto dei sistemisti, si individuano i sistemi potenzialmente interconnessi tra loro (e.g. stesso servizio, DB condiviso, flusso dati tra sistemi), analizzandone le dipendenze ed aggregando, se possibile, i relativi *ticket* nella medesima attività di migrazione;
- **definizione di un piano di *roll-back***: ogni attività di migrazione dettagliata nei singoli *Deployment Plan* deve necessariamente prevedere una procedura di *rollback* che consenta il ripristino dei sistemi al momento precedente l'inizio dell'attività di migrazione:
  - nel caso di migrazione *Physical To Virtual* o *Virtual To Virtual* il *rollback* consiste nella riaccensione dei sistemi di origine, sfruttando, ad esempio, le funzionalità native dello strumento di VMWare HCX, ove applicabili;
  - nel caso di migrazione fisica, i team operativi dovranno mettere in atto tutte le attività necessarie ad evitare che il sistema debba essere rilocato nel luogo di origine. Problemi derivanti da parti *hardware* danneggiate potranno essere risolte grazie al magazzino allestito dai *Vendor* stessi.
- **definizione contatti per escalation**: ogni *Deployment Plan* contiene al suo interno una sezione dedicata all'*Escalation Path* con i contatti dei referenti da coinvolgere in caso debbano essere prese decisioni di rilievo (e.g. estensione del disservizio della CRQ, autorizzazione all'esecuzione del *rollback*);
- **gestione del *ticket* e raccolta approvazioni**: il *layer* di *Change* è responsabile della gestione degli stati delle varie CRQ, dalla fase iniziale a quella di schedulazione, assicurandosi che le CRQ siano registrate, valutate, autorizzate, prioritizzate, pianificate, testate, implementate, documentate e revisionate in modo controllato, garantendo la riposta ai diversi requisiti tecnologici, massimizzando il valore e riducendo *incident*, disservizi e rilavorazioni. Raccoglie e relaziona le varie approvazioni a tutti i *Gate* approvativi, includendo la documentazione tecnica ed il relativo *Deployment Plan* oltre che le comunicazioni effettuate verso i vari *stakeholder*. Il CAB coordina la revisione, l'approvazione o il rifiuto delle attività di migrazione. I *Gate* approvativi sono principalmente due: quello tecnico, con i *team* di *Operations*, e quello con la PA utente;
- **verifica di potenziali *clash***: tutte le attività di migrazione vengono analizzate, tramite l'utilizzo di apposita piattaforma, dal punto di vista degli impatti con altre attività di migrazione o *Business As Usual* ("BAU"). I conflitti vengono quindi evidenziati e risolti modificando le pianificazioni delle CRQ coinvolte;
- **gestione delle comunicazioni con gli *stakeholder* impattati**: il *Change Enablement* gestisce ed effettua le attività di comunicazione verso tutti i *team* operativi coinvolti e tutti i referenti della PA utente, informandoli sullo stato approvativo di ogni attività e comunicando quelle pianificate nell'immediato;
- **verifica delle attività pre-migrazione**: al fine di garantire il buon esito delle migrazioni, il *Change Enablement* si occupa di verificare con i *team* di *Operations* che tutte le attività propedeutiche siano state correttamente eseguite nei modi e tempi concordati:

- *backup*
- predisposizione cablaggi
- aperture di rete
- controllo sovrapposizioni;

- **Coordinamento migrazione**: il *layer* di *Change* effettua il coordinamento delle migrazioni, dettando i tempi di esecuzione, ingaggiando sequenzialmente l'assegnatario di ogni *task* e pre-allertando il successivo. Traccia gli stati di avanzamento rispetto al *Deployment Plan* sul sistema di *ticketing* e, in caso di necessità, attiva il processo di *Escalation Path*;
- **Controllo qualità post-migrazione**: a conclusione della migrazione, il *Change Enablement* effettua gli opportuni controlli per la corretta valutazione dell'esito complessivo dell'attività svolta e dello stato operativo dei sistemi coinvolgendo i referenti applicativi della PA utente. In caso di esito positivo, procede alla chiusura della CRQ; diversamente, procede all'apertura di un *Incident* per tracciare il problema e consentirne una rapida risoluzione.

#### *1.21.4.2 Classificazione delle CRQ*

Nell'ambito delle attività di migrazione si utilizzano diverse classi di CRQ a seconda del livello di criticità dell'attività:

*Tabella 15: Classi delle CRQ*

| Classificazione | Descrizione | Livello di criticità |
|---|---|---|
| Standard | CRQ pre-autorizzate dove il processo di implementazione ed i rischi sono noti in anticipo.<br>Utilizzate prevalentemente per migrazioni *Virtual To Virtual* di ambienti non di produzione. | Basso |
| Normal | Attività che devono seguire l'intero processo di *Change Enablement* e relativa approvazione a *Change Advisory Board* ("CAB").<br>Utilizzate per migrazioni di ambienti fisici e virtuali di produzione. | Medio |
| Emergency | Attività che devono essere implementate urgentemente per risolvere o prevenire *Incident* critici (P1/P2) o per implementare requisiti tecnici o di *business* urgenti.<br>Utilizzate per mitigare problematiche esistenti accelerando il processo approvativo e di migrazione di ambienti di produzione. | Alto |

Tutte le CRQ sono tracciate tramite l'appropriato strumento di gestione *ticket* ITSM.

#### *1.21.4.3 Strumenti di change enablement a supporto delle migrazioni*

Il *layer* di *Change Enablement* utilizza i seguenti strumenti nella gestione delle diverse fasi di svolgimento della migrazione:

- **Strumento di gestione *Ticket* ITSM**: piattaforma centralizzata che traccia i *ticket* aperti ed archivia i dati delle attività già implementate. Per essere lavorati, i *ticket* devono essere tracciati nello strumento di gestione ITSM. Questo assicura che tutti i tipi di richieste siano supportate da un livello appropriato di informazioni e dettagli, tra cciati a livello di *ticket* stesso. Nel caso di molteplici richieste di tipo simile, si crea un *ticket* principale a cui saranno collegate le richieste stesse con relazione genitore-figlio all'interno della soluzione ITSM. Inoltre, qualsiasi *Incident/Problem/Service Request* viene relazionato alle relative CRQ impattate all'interno della soluzione ITSM;

- *Configuration Management Database* (CMDB): *repository* con le informazioni sui *Configuration Items* (CI) che compongono l'infrastruttura IT. Il CMDB include un elenco di elementi sulla configurazione, i relativi attributi e relazioni tra di essi e supporta le fasi di pianificazione delle CRQ di migrazione, permettendo di individuare le relazioni tra i Cis in *scope*;
- Strumento a supporto delle migrazioni e gestione dei *Clash*: le funzioni di rilevamento dei *clash* native nella piattaforma di gestione *ticket* ITSM, o in una piattaforma separata basata su *software Open Source* in grado di fornire questo servizio, vengono utilizzati dalla funzione di *Change Enablement* per identificare in anticipo i potenziali conflitti tra le migrazioni pianificate (*Clash Management*).

#### *1.21.4.4 Strumento a supporto delle migrazioni e di gestione dei clash*

Al fine di ridurre al minimo i rischi di disservizio, tutte le CRQ di migrazione e quelle inerenti alle attività *Business As Usual* ("BAU") sono sottoposte ad un processo d'identificazione dei *clash*. Questo processo convalida la possibile esecuzione delle attività di migrazione verificando che:

- durante il processo di migrazione non siano in esecuzione CRQ che impattino gli stessi CI per *patching*/rilasci applicativi/*reboot* pianificati;
- durante il processo di migrazione non siano in esecuzione CRQ che impattino CI relazionati tra loro a livello applicativo/infrastrutturale;
- durante il processo di migrazione non siano previsti interventi di manutenzione a livello network che possano compromettere l'attività stessa.

Queste funzioni di identificazione *clash* potranno essere erogate dalla piattaforma di *ticketing* se disponibili o tramite una piattaforma *software Open Source* atta allo scopo. La piattaforma fornisce:

- KPI dettagliati ed automatizzati per supportare le attività operative e decisionali. Sono a disposizione ***dashboard*** dedicate a seconda del profilo utente, che forniscono una visione chiara ed esaustiva dell'andamento del progetto, delle *wave* di migrazione e delle singole CRQ. I KPI sono totalmente personalizzabili a seconda del livello di dettaglio desiderato.




*Figura 52: Dashboard dei KPI del tool di Clash management*

- visualizzazioni e *report* dedicati per le funzioni di migrazione e reportistica *ad hoc* per i team di *Operations*. Il sistema è in grado di produrre report aggiornati sulla base della frequenza di *refresh* del sistema di *ticketing* ed inviarli automaticamente alle *distribution*

*list* configurate. Anche in questo caso il livello di dettaglio dei *report*, lo *scope* ed i campi visualizzati saranno totalmente personalizzabili sulla base dei differenti destinatari;

- un motore di rilevamento dei conflitti parametrizzabile con differenti regole che permette l'identificazione e la visualizzazione automatica delle attività che richiedono l'attenzione del *Change Enablement* al fine di risolvere i ***clash***. I parametri utilizzabili per l'identificazione dei conflitti saranno totalmente personalizzabili tra CI, *location*, servizi di appartenenza, piattaforme impattate, periodi di *freeze* programmati;



*Figura 53: Dashboard di rilevazione dei conflitti*

- *dashboard tracker* di migrazione che, fornendo una visione complessiva di tutte le attività pianificate (migrazioni, BAU, *freeze*, canvas, rilasci), supporta il *Change Enablement* nell'identificazione di eventuali slot temporali disponibili al fine di ottimizzare la pianificazione e sfruttare al meglio le finestre temporali a disposizione.

Nel caso di migrazioni molto complesse che coinvolgono PA di grandi dimensioni, si ritiene ottimale l'utilizzo dello strumento HPE *Right Mix Advisor* che supporta la pianificazione delle attività, secondo il seguente processo:

- *discovery* automatica delle applicazioni e dei sistemi da migrare;
- Integrazione dei dati raccolti con le risposte a questionari sottoposti ai vari gruppi operativi;
- definizione del piano di migrazione di alto livello con identificazione delle applicazioni coinvolte nella prima *wave* di migrazione (applicazioni che presentano un ridotto numero di dipendenze e non richiedono attività di trasformazione);
- determinazione degli approcci di migrazione in relazione al paradigma delle 6R, ed individuazione delle possibili piattaforme *target*.

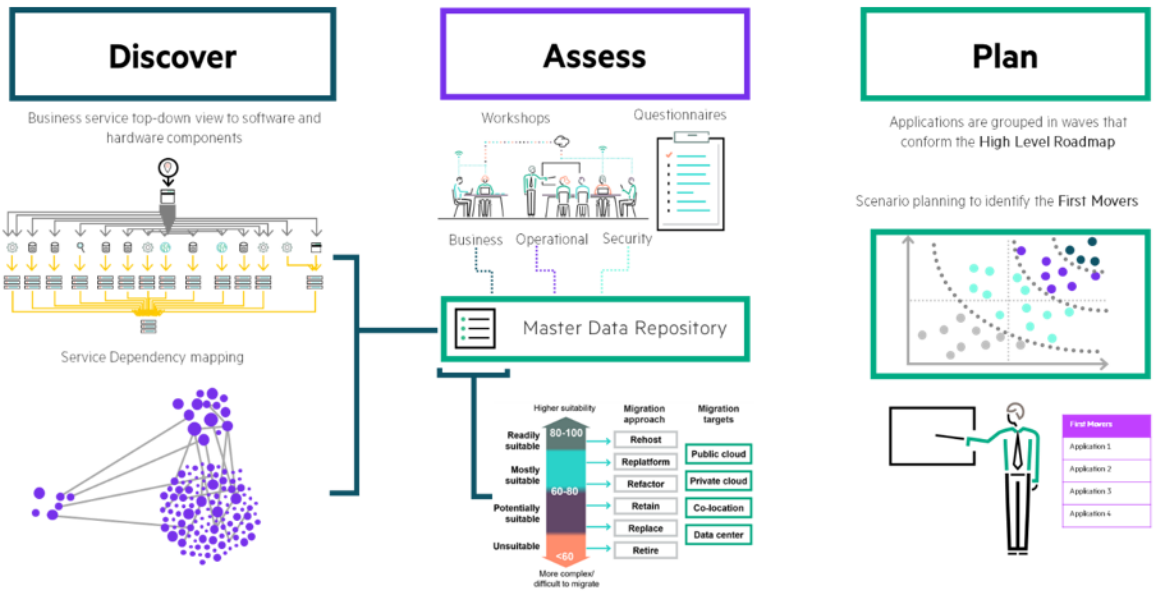



*Figura 54: Vista dello strumento HPE Right Mix Advisor*

### 1.21.5 Strumenti a supporto della migrazione

Si fornisce una panoramica degli strumenti che la NewCo potrebbe utilizzare a supporto della migrazione, con la distinzione degli strumenti utili alla fase transitoria, e quelli utili alla migrazione dei dati.

Gli strumenti menzionati non vogliono rappresentare una lista esaustiva ma esemplificativa, in quanto la scelta definitiva avverrà in fase di valutazione del modello di trasformazione da adottare, secondo specifica analisi dei requisiti ed attenta valutazione dell'offerta presente sul mercato.

#### *1.21.5.1 Strumenti a supporto della fase transitoria*

È corretto e opportuno ipotizzare che per molte delle soluzioni della PA utente installate *on-premise*, la migrazione non possa avvenire in modalità *switch-off*, *switch-on*; con alta probabilità, la migrazione potrebbe richiedere una fase transitoria, durante la quale alcune componenti continueranno ad essere erogate nel contesto originale, mentre altre verranno progressivamente migrate verso la NewCo. Particolarmente critici risultano i casi in cui vi siano forti interdipendenze tra i moduli in fase di migrazione ed i moduli per cui la migrazione è pianificata in fasi successive.

In questo scenario, risulta fondamentale dotarsi di strumenti che garantiscano la *Business Continuity* consentendo la migrazione in modalità *safe*, senza creare lunghi periodi di indisponibilità del servizio erogato.

Tra i possibili *tool*, in particolare relativamente alla casistica di migrazione da VMWare, *Bare Metal* o KVM verso tecnologia VMWare, possiamo citare VMWare HCX e vRealize Network Insights (vRNI). L'utilizzo di tali strumenti permette di pianificare una migrazione progressiva delle componenti applicative tenendo conto delle loro interdipendenze e con le caratteristiche di consistenza e disponibilità del servizio tipiche di una operazione di *vMotion* (migrazione a caldo senza disservizio), andando a replicare al contempo le macchine virtuali, il loro contenuto e la configurazione di rete di partenza.

In fase di pianificazione della migrazione, infatti, utilizzando il *tool* VMWare vRNI, è possibile individuare e mappare le interdipendenze tra le varie applicazioni, siano esse erogate tramite *Virtual Machine* o *Bare Metal*, e pianificare una migrazione consistente di tutti i moduli applicativi.

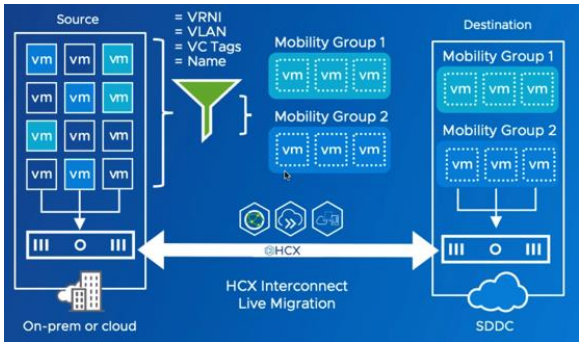



*Figura 55: Funzionamento dello strumento HCX*

### *1.21.5.2 Strumenti a supporto della migrazione dei dati*

Su eventuale richiesta della PA utente, si prevede di supportare migrazioni applicative parziali, per un periodo di tempo limitato alla fase di migrazione dei DC della PA utente.
Per migrazioni applicative parziali si intendono quei sistemi afferenti al medesimo ambito, per i quali valgono entrambe le seguenti condizioni:

- parti delle componenti applicative ed i relativi dati permangono per un tempo anche prolungato sui sistemi sorgente;
- parti delle componenti applicative vengono migrati su infrastrutture del PSN e devono poter accedere ai dati immagazzinati nell'ambiente originario.

In queste casistiche, è necessario garantire un flusso di dati da e verso i moduli ospitati su infrastruttura della NewCo che sia: continuo, consistente, non bloccante.
A tale fine, è importante l'utilizzo di modalità di disaccoppiamento della comunicazione basate su paradigmi *Producer/Consumer* o *Publisher/Subscriber*, mediante l'introduzione di tecnologie basate su *Message Bus*. Un esempio notevole, e standard *de facto* in tal senso, è rappresentato da *Apache Kafka* e dall'ecosistema costituito dai *tool* di *Change Data Capture* (e.g. Connect) ad esso collegati (alcuni esempi di connettori molto utilizzati: SQL DB to Kafka, File to Kafka, Kafka to SQL DB, MongoDB to Kafka, Kafka to MongoDB, Kafka to S3…).
Ai fini di un *enforcement* di sicurezza, si ipotizza di utilizzare un livello di *encryption in-transit* per tutti i dati che transitano all'interno del *Message Bus* ed un livello di *encryption at rest* per tutti i dati persistiti su *storage*. Entrambi gli scenari sono supportati nativamente dal prodotto Apache Kafka citato in esempio.
Terminata la fase di migrazione, tale tecnologia potrebbe rimanere, su richiesta, a disposizione dell'infrastruttura della NewCo, nell'ottica di facilitare e supportare la transizione applicativa verso modelli architetturali *cloud native*, soprattutto durante le fasi di *Replatform* e *Rearchitect*.
La migrazione dei dati è particolarmente complessa in presenza delle seguenti situazioni:

- dati afferenti a sistemi che girano su infrastrutture *legacy* caratterizzate da paradigmi di sicurezza obsoleti;
- PA utenti di grandi dimensioni e quindi grande mole di dati da trasferire via rete, per cui i tempi di migrazione non sono compatibili con le tempistiche di piano;
- PA utenti di piccole dimensioni, dotate di banda discontinua o insufficiente a garantire la piena operatività dei servizi durante la copia dei dati.

In queste casistiche, ad esempio, l'Offerente propone l'utilizzo di una soluzione ingegnerizzata col *partner* HPE che include:

- *l'hardware* necessario alla migrazione, comprensivo di *storage*;
- il prodotto *leader* di mercato Zerto, in grado di eseguire *backup point in time* di singole VM o di gruppi di VM in modo agnostico rispetto al tipo di *storage* sottostante.

Questa soluzione permette di estrarre i dati da migrare direttamente presso il DC della PA utente, cifrarli con una chiave fornita dalla stessa, e di trasportarli e ripristinarli sui sistemi della NewCo.
In questo modo, si garantisce la massima velocità di copia, la massima sicurezza e la consistenza dei dati sottoposti a *backup*, in particolare riducendo l'esposizione a potenziale compromissione di dati non cifrati.

## 1.22 ID CRITERIO:22 – VALUTATIVO - MIGLIORAMENTI DELLA STRATEGIA DI MITIGAZIONE DEI RISCHI CONNESSI ALLA MIGRAZIONE DEI SERVIZI DELLE AMMINISTRAZIONI (DISPONIBILITÀ, INTEGRITÀ E PERFORMANCE)

| ID | Tipologia | Categoria | CRITERIO | DESCRIZIONE DEL CRITERIO | PUNTEGGIO TOTALE MASSIMO CONSEGUIBILE |
|---|---|---|---|---|---|
| 22 | Valutazione | Migrazione | Mitigazione dei rischi connessi alla migrazione *cloud* | Miglioramenti della strategia di mitigazione dei rischi connessi alla migrazione dei servizi delle amministrazioni (disponibilità, integrità e performance) | **4** |

Questa sezione descrive i miglioramenti proposti dall'Offerente in merito alla **mitigazione dei rischi connessi alla migrazione** dei servizi della PA utenti.

### 1.22.1 Analisi dei rischi e mitigazione

Si riportano di seguito i principali rischi associati alle attività di migrazione e l'approccio che si intende intraprendere per la mitigazione. Si riportano a puro titolo esemplificativo gli strumenti che possono abilitare le azioni di mitigazione delineate:

*Tabella 16: Rischi di migrazione ed azioni di mitigazione*

| Rischio | Mitigazione e Strumento |
|---|---|
| Disservizi per conflitti fra diverse attività di migrazione | Utilizzo di uno strumento di *clash Management* che identifichi CRQ in conflitto o CRQ impattanti gli stessi servizi o CRQ non allineate con eventi di *freezing* |
| Inefficienze dovute a servizi coesistenti su molteplici ambienti | Utilizzo di uno strumento (quale HCX di VMware) che gestisca la migrazione progressiva delle componenti applicative, considerandone le interdipendenze |
| Prolungamento dei tempi di migrazione a causa di interruzioni nel trasferimento di dati per connettività discontinua | Utilizzo di un *Message Bus* (i.e. Apache Kafka) per il *buffering* dei dati in transito verso il PSN, che sfrutta efficientemente gli intervalli di piena connettività e la banda disponibile |
| Perdita di dati dovuta a connettività discontinua o banda non sufficiente | Utilizzo di un sistema ingegnerizzato fornito dalla NewCo in collaborazione con i propri *partner*, che fornisce *l'hardware* necessario a supportare la migrazione ed il *software* che orchestra la copia, la cifratura ed il ripristino dei dati |
| Tempi di migrazione non compatibili con le esigenze della PA utente, per grandi quantitativi di dati da trasferire via rete | |

| | |
|---|---|
| Compromissione di dati non cifrati relativi a sistemi *legacy* durante il trasporto del *rack* | |

Si rimanda ai paragrafi 1.21.4.4 e 1.21.5 per maggiori dettagli.

### 1.22.2 Analisi di Sicurezza

La NewCo, sulla base degli interventi di migrazione, adotterà **diverse strategie di messa in sicurezza** dei dati memorizzati sull'infrastruttura, **differenziandole** in base alla modalità di migrazione, alla rilevanza ed alla classificazione delle informazioni gestite.
L'approccio proposto dall'Offerente prevede la fornitura di diverse *capability* di protezione, che saranno poi valutate dalle PA utenti e potranno essere applicate con un principio di proporzionalità rispetto a requisiti di sicurezza ed impatti/costi in fase di migrazione.
In tutti gli scenari che prevedono la trasformazione della piattaforma esistente (dal *rehost* al *rearchitect*) saranno applicate misure di protezione atte a garantire il principio di ***security by design,*** che permette di implementare controlli a priori in modo da massimizzarne il beneficio e ridurre i relativi costi di realizzazione. Tali misure sono strettamente collegate alle modalità di migrazione ed al tipo d'interventi realizzativi della nuova infrastruttura (es. ridefinizione dell'architettura applicativa e dei segmenti di rete per la gestione dei diversi componenti infrastrutturali).
Le misure di sicurezza proposte sulla base della strategia di migrazione applicata sono riportate nella seguente tabella.

*Tabella 17: Misure di Sicurezza per strategia di migrazione*

| | | Remain (Housing) | Rehost | Replatform | Refactor | Revise | Rearchitect |
|---|---|---|---|---|---|---|---|
| Data In transit | **Mezzi blindati con scorta** | ✓ | N/A | N/A | N/A | N/A | N/A |
| | **Applicazione di sigilli ai rack e/o ai container dei server durante il trasporto** | ✓ | N/A | N/A | N/A | N/A | N/A |
| | **Adozione di protocolli sicuri per il trasferimento dati** | N/A | ✓ | ✓ | ✓ | ✓ | ✓ |
| Data at rest | **Protezione dei dati *at-rest* mediante cifratura con chiavi gestite direttamente dalla PA utente, o laddove richiesto da parte della NewCo** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security by design | **Security testing al termine della migrazione** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ***Hardening dell'hypervisor* e dei sistemi operativi guest** | N/A | ✓ | N/A | N/A | ✓ | N/A |
| | **Utilizzo di template di *hardening* per l'infrastruttura *cloud*** | N/A | N/A | ✓ | ✓ | N/A | ✓ |
| | **Revisione del codice in ottica di sviluppo sicuro** | N/A | N/A | N/A | N/A | ✓ | ✓ |
| | **Attivazione di regole di *logging*** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | **Gestione utenze privilegiate** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Il simbolo ✓ riporta le misure messe a disposizione dalla NewCo e fortemente raccomandate, sulla base dello scenario di migrazione, al fine di garantire gli obiettivi di protezione rispetto ai seguenti ambiti:

- protezione dei dati durante il trasferimento;
- protezione dei dati memorizzati sui sistemi migrati all'interno del PSN;
- applicazione dei principi base di *security by design* per garantire una *baseline* di protezione comune dell'infrastruttura e dei dati.

Sulla base dello scenario di migrazione e della criticità dei sistemi e dei dati relativi, le PA utenti potranno stabilire le misure di sicurezza da applicare, fermi restando i vincoli normativi a cui sono soggette nell'ambito della gestione dei dati. Ulteriori misure di sicurezza, proposte dalle PA utenti alla NewCo in fase di migrazione, potranno essere valutate e prese in considerazione puntualmente per garantire il rispetto delle esigenze di sicurezza delle singole PA utenti.

Roma, 21 Marzo 2022

Augusto Di Genova
Fastweb - Chief Enterprise Officer

_____

Gaetano Paolino
Fastweb - Head of Central Government

_____

Susanna Santini
Aruba - Presidente

_____

**GARA EUROPEA, A PROCEDURA APERTA, PER L'AFFIDAMENTO, MEDIANTE UN CONTRATTO DI PARTENARIATO PUBBLICO-PRIVATO, DELLA REALIZZAZIONE E GESTIONE DEL POLO STRATEGICO NAZIONALE**

**CIG: 9066973ECE**

**CUP: J51B21005710007**

# Relazione Tecnica Illustrativa

21 marzo 2022

Rev. 1.0

## Sommario

1 Premessa ..... 13
2 Presentazione del costituito RTI ..... 15
2.1 TIM S.p.A. ..... 15
2.2 CDP Equity S.p.A. ..... 16
2.3 Leonardo S.p.A. ..... 17
2.4 Sogei S.p.A. ..... 19
3 ID 1 – Tabellare - Miglioramento del PUE misurato su base annuale per ciascun anno e per ciascun Data Center a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 1,5 ..... 21
4 ID 2 – Tabellare - Miglioramento della % di approvvigionamento elettrico da fonti rinnovabili anche ai fini dell'indipendenza energetica per il relativo approvvigionamento misurato per ciascun Data Center su base annuale per ciascun anno a partire dal secondo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 50% ..... 21
5 ID 3 – Tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di informazioni personali, quali certificazioni della famiglia ISO/IEC 29100 oppure ISO/IEC 27701 ..... 22
6 ID 4 – Tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di incidenti di sicurezza, quali la ISO 27035. ..... 22
7 ID 5 – Tabellare - Incremento del numero di fornitori di servizi di public cloud (CSP qualificati) rispetto al valore base della proposta pari a 3 con i quali il concorrente si impegna a far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: Public Cloud PSN Managed, Secure Public Cloud, Hybrid Cloud on PSN Site ..... 22
8 ID 6 – Tabellare - Miglioramento dell'offerta di servizi cloud mediante utilizzo di tecnologia Open Source. Per tali servizi, l'offerta tecnica deve prevedere la descrizione della componente tecnica e la descrizione delle tempistiche di disponibilità di tali servizi che saranno inseriti in sede di aggiornamento del listino prezzi, comunque non oltre i 2 anni dalla sottoscrizione della Convenzione ..... 23
8.1 Piattaforma per container (CaaS) basata su tecnologia Open Source OKD ..... 24
8.2 Piattaforma per collaboration basata su tecnologia Open Source Mattermost ..... 29
9 ID 7 – Tabellare - Miglioramento del valore soglia dell'indicatore di qualità IQ04 pari a numero 5 rilievi ..... 32
10 ID 8 – Tabellare - Miglioramento dei seguenti valori: - RTO atteso dell'indicatore di qualità IQ11 pari a 30 minuti - RPO target dell'indicatore di qualità IQ12 pari a 1 minuto - RTO su diversa

Region atteso dell'indicatore di qualità IQ13 pari a 4 ore - RPO su diversa Region target dell'indicatore di qualità IQ14 pari a 30 minuti ..... 32

11 ID 9 – Tabellare - Miglioramento dei valori soglia dell'indicatore di qualità IQ017 con riferimento ai tempi massimi di risoluzione in ore (Priorità 1 <= 4 ore; Priorità 2 <= 8 ore; Priorità 3 <= 12 ore ..... 32

12 ID 10 – Tabellare - Riduzione sul periodo minimo di disponibilità dell'infrastruttura di 180 giorni. Il cronoprogramma dovrà evidenziare tutti gli step relativi alla disponibilità dell'infrastruttura evidenziando le proposte che presentino la maggior celrità realizzativa ..... 33

13 ID 11 – Tabellare - Possesso, in capo al concorrente singolo o associato, della certificazione di responsabilità sociale ed etica SA 8000 o equivalente ..... 33

14 ID 12 – Tabellare - Impiego o assunzione di persone con disabilità in quota eccedente l'obbligo minimo di legge, nell'organico della società di progetto (NewCo) ..... 35

15 ID 13 – Tabellare - Componente lavoro femminile superiore al 10% dell'organico della società di progetto (NewCo) ..... 36

16 ID 14 – Tabellare - Componente lavoro giovanile (età inferiore a 36 anni) superiore al 5% dell'organico della società di progetto (NewCo) ..... 36

17 ID 15 – Valutativo - Efficacia delle modalità di verifica proposte dal Concessionario, messe a disposizione del concedente, per il rispetto delle seguenti norme e standard europei in materia ambientale (Do no significant harm): - ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD(2020) 55 final); - Indipendenza energetica e fonti rinnovabili; - Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE); - Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva; - Le procedure di approvvigionamento includeranno la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali; - Al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della direttiva 2012/19/UE ..... 37

17.1 Executive Summary ..... 37

17.2 ISO 50001 ..... 38

17.3 PUE ..... 39

17.4 EN 50600 ..... 41

17.5 ISO 14064 ..... 41

17.6 ISO 14001 ..... 46

17.7 SWD (2020) 55 final ..... 47

17.8 Indipendenza energetica e fonti rinnovabili ..... 49

17.9 Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE) ..... 50

17.10 Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva (Direttiva RoHS) ..... 54

17.11 Procedure di approvvigionamento e Gestione del ciclo di vita delle apparecchiature .60

18 ID 16 – Valutativo - Miglioramenti, a favore del Concedente, della matrice di ripartizione del rischio. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili ..... 63

18.1 Executive Summary ..... 63

18.2 Rischio “Domanda” ..... 64

18.3 Rischio “Forza Maggiore” ..... 66

18.4 Rischio “Mutamenti imposti ex lege” ..... 66

19 ID 17 – Valutativo - Miglioramenti del modello di governance utili a consentire un maggior coinvolgimento del Concedente anche nell'ottica di garantire ulteriormente la vigilanza e il monitoraggio pubblico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili ..... 67

19.1 Executive Summary ..... 67

19.2 Governance ..... 67

19.3 Governo della Convenzione e figure a supporto ..... 69

19.4 Comitati ..... 70

19.5 Funzioni di staff ..... 73

19.6 Piano di comunicazione ..... 76

19.7 Processi / Interazioni con il Concedente e ciascuna Amministrazione aderente e con i Fornitori Terzi ..... 78

19.8 Strumenti a supporto dell’organizzazione ..... 82

20 ID 18 – Valutativo - Miglioramenti, a favore del Concedente, della compliance nell’aggiornamento dei costi e prezzi dell’infrastruttura anche da un punto di vista del refresh tecnologico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili ..... 90

20.1 Executive summary ..... 91

20.2 Modalità operative per il controllo dei costi ed il refresh tecnologico ..... 92

20.3 Modalità operative per la revisione dei prezzi ..... 95

20.4 Cronoprogramma della Convenzione ..... 98

21 ID 19 – Valutativo - Miglioramenti sulla proposta progettuale per quanto riguarda gli aspetti relativi all'integrazione del PSN con l'Architettura Nazionale Cyber, con particolare riguardo alle modalità ed ai processi per l'integrazione con lo CSIRT Italia (fino a 1 punto), alla messa a disposizione di funzionalità per l'interazione con gli ISACs (fino a 1,5 punti), messa a disposizione di funzionalità di per scambio di informazioni A2A tra il SOC e lo CSIRT Italia (fino a 1,5 punti) 99

21.1 Executive Summary ..... 99

21.2 Processi per l'integrazione con l'Architettura Nazionale di sicurezza e lo CSIRT Italia 101

21.3 Funzionalità A2A per scambio di informazioni con il CSIRT Italia ..... 110

21.4 Funzionalità per l'interazione con gli ISACs ..... 114

22 ID 20 – Valutativo - Completezza, accuratezza e verificabilità del metodo che il concorrente si impegna ad adottare per la definizione del dimensionamento delle risorse (giorni/uomo e relativo team mix per tipologia di strategia di migrazione) e delle tempistiche per la realizzazione di ciascuna fase di ciascun progetto di migrazione per gli scenari 1, 2 e 3 e per i casi di "breve termine" e "medio e lungo termine" ..... 117

22.1 Executive Summary ..... 117

22.2 Approccio metodologico al dimensionamento risorse e tempistiche del Piano di Migrazione ..... 118

22.3 Dimensionamento e Tempistiche per la Fase di Analisi/Discovery ..... 120

22.4 Dimensionamento e Tempistiche per le Fasi di Setup/Migrazione/Collaudo ..... 124

22.5 Use Case ..... 131

22.5.1 Use Case 1 – "Best Case" ..... 132

22.5.2 Use Case 2 – "Worst Case" ..... 133

22.5.3 Use Case 3 – "Mixed Case" ..... 133

22.6 Approccio metodologico per l'esecuzione delle fasi di Migrazione ..... 134

22.6.1 EXPLORE - Fase di Analisi/Discovery ..... 138

22.6.2 MAKE - Fase di Setup ..... 149

22.6.3 MAKE - Fase di Migrazione ..... 150

22.6.4 GO - Fase di Collaudo ..... 152

23 ID 21 – Valutativo - Miglioramenti del modello organizzativo, delle metodologie e degli strumenti che il concorrente si impegna ad adottare per il monitoraggio e il controllo della migrazione al fine del rispetto delle tempistiche previste ..... 154

23.1 Executive Summary ..... 154

23.2 Modello Organizzativo ..... 155

23.2.1 Modello Organizzativo per la gestione delle attività di governance e delle attività operative ..... 155
23.2.2 Dettaglio ruoli del modello organizzativo ..... 156
23.2.3 Protocolli di Comunicazione ..... 159
23.3 Metodologie ..... 161
23.3.1 Gestione del Portfolio ..... 162
23.3.2 Monitoraggio e Controllo del Progetto ..... 163
23.3.3 Monitoraggio delle Performance del Progetto ..... 164
23.3.4 Gestione dei rischi ..... 167
23.3.5 Change Management e Formazione ..... 167
23.3.6 Gestione della flessibilità organizzativa ..... 168
23.4 Strumenti ..... 172
23.4.1 Masterplan ..... 173
23.4.2 Planner risorse ..... 173
23.4.3 Piano di Progetto ..... 174
23.4.4 Cruscotto Monitoraggio Avanzamento ..... 175
23.4.5 Issue Log ..... 176
23.4.6 Tool e Tecnologie di Migrazione ..... 176
23.4.7 KPI Monitoring Dashboard ..... 177
23.4.8 Piano di Change Management ..... 178
23.4.9 Report di Change Management ..... 178
24 ID 22 – Valutativo - Miglioramenti della strategia di mitigazione dei rischi connessi alla migrazione dei servizi delle amministrazioni (disponibilità, integrità e performance) ..... 178
24.1 Executive Summary ..... 178
24.2 Misure di Mitigazione ..... 182
24.2.1 Misure di mitigazione adottate per ciascuna fase della migrazione ..... 184
24.2.1.1 Analisi/Discovery ..... 184
24.2.1.2 Setup ..... 186
24.2.1.3 Migrazione ..... 187
24.2.1.4 Collaudo ..... 188
24.2.1.5 Test di Performance ..... 190
24.2.1.6 Test di Disponibilità ..... 191

24.2.1.7 Test di Integrità ..... 191
24.2.1.8 Test di Funzionalità ..... 192
24.2.2 Misure di mitigazione adottate nella fase di Post Migrazione ..... 193
24.2.2.1 Source shutdown ..... 193
24.2.2.2 Condivisione e consolidamento della Knowledge Acquisita nella Migrazione 194
24.3 Risk Management ..... 195
24.3.1 Metodologia ..... 195
24.3.2 Struttura Organizzativa ..... 197
24.3.3 Strumenti ..... 198
24.3.3.1 Risk Management Plan ..... 198
24.3.3.2 Risk Register ..... 199
24.3.3.3 Mitigation Plan ..... 200
24.3.3.4 Contingency Plan ..... 200
24.3.3.5 Report ..... 201
24.3.3.6 Cruscotti ..... 202
24.4 Risk analysis ..... 203
24.4.1 Livello rischio potenziale ..... 203
24.4.2 Livello rischio residuo ..... 204
24.4.3 Rischio effettivo ..... 206
25 Allegati ..... 207

## Indice delle Figure

Figura 1 DC Region Nord ..... 14
Figura 2 DC Region Sud ..... 14
Figura 3 Architettura OCI ..... 26
Figura 4 Strumenti chiave Mattermost ..... 29
Figura 5 Esempi interfaccia utente ..... 30
Figura 6 Direttiva 2009/125/CE ..... 51
Figura 7 Esempio di scoring ..... 59
Figura 8 Macro-flusso - Reborn HW ..... 62
Figura 9 Matrice dei rischi ..... 64
Figura 10 Modello di Governance ..... 68
Figura 11 Modello Organizzativo ..... 69
Figura 12 Comitati a livello di Convenzione ..... 71
Figura 13 Comitato di Contratto di Adesione ..... 72
Figura 14 Piano di comunicazione ..... 76
Figura 15 Piano di Comunicazione ..... 77
Figura 16 Macro-processo di Governance ..... 79
Figura 17 Attori coinvolti ..... 87
Figura 18 Esempio di vista Data Center ..... 89
Figura 19 Esempio vista Mappa ..... 90
Figura 20 Processo di adeguamento prezzi, costi e tecnologie ..... 92
Figura 21 Check identificativi ..... 93
Figura 22 Modalità operativa del Concessionario ..... 95
Figura 23 Fasi di fornitura ..... 98
Figura 24 Architettura Nazionale Cyber ..... 101
Figura 25 Interazione tra PSN e autorità istituzionali nell'ambito della cybersicurezza ..... 105
Figura 26 Organizzazione ufficio di sicurezza PSN e processi CSIRT ..... 108
Figura 27 Diamond Model ..... 111
Figura 28 Knowledge Base di Sicurezza e piattaforma TIP ..... 113
Figura 29 Form di comunicazione incidenti al CSIRT Italia ..... 114
Figura 30 MISP Dashboard ..... 115
Figura 31 TLP e restrizioni ..... 116
Figura 32 Framework EMG2C ..... 117
Figura 33 Fasi del progetto di migrazione ..... 119
Figura 34 Landing zone per livello di maturità ..... 125
Figura 35 Matrice di complessità ..... 126
Figura 36 Framework metodologico ..... 135
Figura 37 Approccio metodologico ..... 137
Figura 38 Step 1 - Assessment ..... 140
Figura 39 Processo di classificazione dati e servizi digitali ..... 146
Figura 40 Step 2 - Definizione Strategia di Migrazione ..... 147
Figura 41 Step 3 - Progettazione e Pianificazione Migrazione ..... 147
Figura 42 Modello organizzativo per la gestione delle attività di migrazione ..... 156
Figura 43 Metodologia adottata per le diverse fasi ..... 162

Figura 44 Processo di verifica dell'avanzamento progettuale....164
Figura 45 Approccio per il Change Management e la formazione....168
Figura 46 MasterPlan iniziative esemplificativo....173
Figura 47 Pesi relativi per le varie fasi di migrazione....175
Figura 48 Cruscotto monitoraggio avanzamento....175
Figura 49 Issue Log e strategie di risposta....176
Figura 50 Dashboard di monitoraggio KPI esemplificativa....177
Figura 51 Piano di Change esemplificativo....178
Figura 52 Mappa concettuale....179
Figura 53 Focus Misure di Mitigazione....182
Figura 54 Relazione tra i rischi....183
Figura 55 Focus Fase di Migrazione....184
Figura 56 Focus fase di Post Migrazione....193
Figura 57 Focus Metodologia....195
Figura 58 Processo di Risk Management....195
Figura 59 Focus Struttura Organizzativa....197
Figura 60 Focus Strumenti....198
Figura 61 Focus Livello rischio potenziale....203
Figura 62 Focus Livello rischio residuo....204
Figura 63 Focus Rischio effettivo....206

# Indice delle Tabelle

Tabella 1 Illustrazione report periodici ..... 41
Tabella 2 Funzioni di staff ..... 74
Tabella 3 Checkpoint - Frequenza ..... 79
Tabella 4 Checkpoint aggiuntivi - Frequenza ..... 81
Tabella 5 Vantaggi del portale ..... 87
Tabella 6 KPI interni per misurazione dei parametri ..... 94
Tabella 7 Rappresentazione dei colori in base alle differenze percentuali ..... 97
Tabella 8 Processi di comunicazione con le istituzioni ..... 105
Tabella 9 Dettaglio dei ruoli del modello organizzativo ..... 156
Tabella 10 Dettaglio dei protocolli di comunicazione ..... 159
Tabella 11 Esempi di KPI per monitoraggio della performance di progetto ..... 165
Tabella 12 Processo di gestione e controllo delle criticità ..... 169
Tabella 13 Strumenti per gestione e monitoraggio della fornitura ..... 172
Tabella 14 Modello di mitigazione del rischio ..... 183
Tabella 15 Legenda valutazione impatti ..... 184
Tabella 16 Valutazione impatti Analisi/Discovery ..... 186
Tabella 17 Valutazione impatti Setup ..... 186
Tabella 18 Valutazione impatti Migrazione ..... 187
Tabella 19 Valutazione impatti Collaudo ..... 189
Tabella 20 Valutazione impatti Post Migrazione ..... 193
Tabella 21 Documentazione per fase di processo Risk Management ..... 196
Tabella 22 Mappatura strumenti per fasi del processo di Risk Management ..... 198
Tabella 23 Mappatura degli strumenti di Risk Management ..... 202
Tabella 24 Criteri per valutazione probabilità accadimento ..... 203
Tabella 25 Matrice Livello di Esposizione ..... 205
Tabella 26 Matrice Livello di Esposizione Rischio Residuo ..... 205

| Glossario |
|---|
| **A** |
| AgID = Agenzia per l'Italia Digitale |
| **C** |
| CA = Contratto di Adesione |
| CD = Continuous Delivery |
| CDC = Comitato di Controllo |
| CDN = Content Delivery Network |
| CI = Continuous Integration |
| CaaS = Container as a Service |
| **D** |
| DB = Database |
| DBaaS = Database as a Service |
| DC = Data Center |
| DEC = Direttore dell'Esecuzione del Contratto |
| DPIA = Data Protection Impact Assessment |
| DR = Disaster Recovery |
| DTD = Dipartimento per la Trasformazione digitale della Presidenza del Consiglio dei Ministri. Alcune volte è indicato come MITD |
| **E** |
| EA = Enterprise Architecture |
| eNPS = Employer Net Promoter Score |
| ESG = Environmental, Social and Governance |
| **G** |
| GO = Garanzia d'Origine |
| GSE = Gestore Servizi Energetici |
| **H** |
| HW = Hardware |
| **I** |
| IaaS = Infrastructure as a Service |
| IDE = Integrated Development Environment |
| IoC = Indicator of Compromise |
| IOPS = Input/Output Operations Per Second |
| ISV = Independent Software Vendor |
| ITIL = Information Technology Infrastructure Library |
| **K** |
| KB = Knowledge Base |
| **M** |
| MITD = Ministro dell'Innovazione Tecnologica e della Transizione Digitale |
| MOL = Margine Operativo Lordo |
| **N** |
| NAS = Network-Attached Storage |
| **P** |

| |
|---|
| PaaS = Platform as a Service |
| PEF = Piano Economico Finanziario |
| PGP = Pretty Good Privacy |
| PM = Project Manager |
| PMBOK = Project Management Body of Knowledge |
| PMCA = PM di Contratto Adesione |
| PMO = Project Management Office |
| POD = raccolta di container Linux che condividono le stesse risorse di calcolo |
| PPAA = Public Procurement Appeals Authority |
| **R** |
| RAV= Replication Assisted vMotion |
| RBAC = Role-Based Access Control |
| RDC = Referente per la Diffusione della Convenzione |
| RoHS = Restriction of Hazardous Substances (Normativa Comunità Europea 2002/95/CE) |
| RPO = Recovery Point Objective |
| RPM = Red Hat Package Manager |
| RTO = Recovery Time Objective |
| RUP = Responsabile Unico del Procedimento |
| **S** |
| SaaS = Software as a Service |
| SAL = Stato di Avanzamento Lavori |
| SAN = Storage Area Network |
| SLA = Service Level Agreement |
| STIX = Structured Threat Information eXpression |
| SW = Software |
| **T** |
| TAXII = Trusted Automated eXchange of Intelligence Information |
| TIR = Tasso Interno di Rendimento |
| **U** |
| UAT = User Acceptance Testing |
| **V** |
| VM = Virtual Machine |

# 1 Premessa

Il presente documento rappresenta la risposta tecnica che illustra la soluzione individuata dal costituito Raggruppamento Temporaneo di Imprese, nel seguito denominato "costituito RTI", formato dalle società TIM S.p.A. (mandataria), CDP Equity S.p.A., Leonardo S.p.A. e SOGEI S.p.A. (mandanti), per l'affidamento, mediante un contratto di partenariato pubblico-privato, della realizzazione e gestione del Polo Strategico Nazionale.

La soluzione proposta risponde ai requisiti espressi nella documentazione di gara che si intendono tutti compresi e accettati. In particolare, il costituito RTI, in qualità di soggetto "Promotore" dello "studio di fattibilità", conferma che la propria soluzione rispetta le specifiche riportate nel paragrafo 5.1 "Determinazione caratteristiche del macrosistema Data Center" a pagina 127 del "progetto di fattibilità".

Sono qui riportate per completezza le informazioni relative a:

- la posizione dei quattro Data Center:
  - Acilia (RM) – Via di Macchia Palocco 223
  - Pomezia (RM) – Strada statale Pontina km29,100;
  - Rozzano (MI) – Via Toscana 3/5;
  - Santo Stefano al Ticino (MI) – Via Ticino 64
- la configurazione in doppia Region dei Data Center:
  - I DC di Acilia e Pomezia compongono la Region sud;
  - I DC di Rozzano e Santo Stefano al Ticino compongono la Region nord;
  - Le due Region distano almeno 500 km l'una dall'altra
- le condizioni di rischio delle aree in cui sono ubicati:
  - I DC utilizzati per ospitare le infrastrutture per il PSN sono tutti certificati Uptime Institute Tier IV e/o ANSI/TIA rating 4, secondo quanto riportato nel Progetto di Fattibilità e ubicati in zone sismiche 3 (ossia zone in cui i forti terremoti sono meno probabili rispetto alla zona 1 e 2)
- le connessioni in fibra ottica realizzate per i collegamenti intra Region:
  - I DC di ogni Region distano almeno 5 km in linea d'aria e sono collegati da percorsi in F.O. completamente diversificati, con lunghezza non superiore a 60km. L'immagine seguente mostra i tracciati in F.O. delle due Region evidenziando la completa diversificazione.

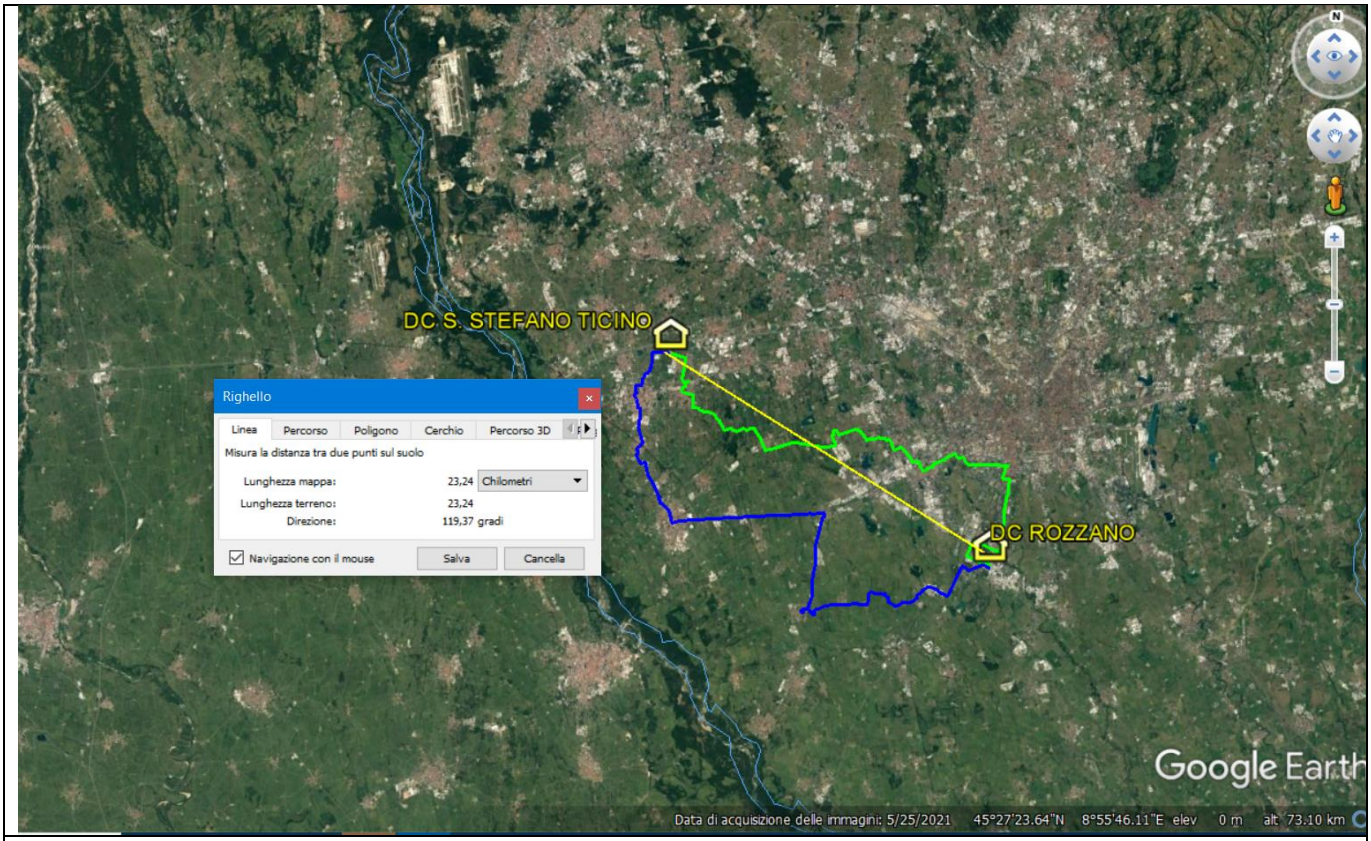



**Figura 1 DC Region Nord**

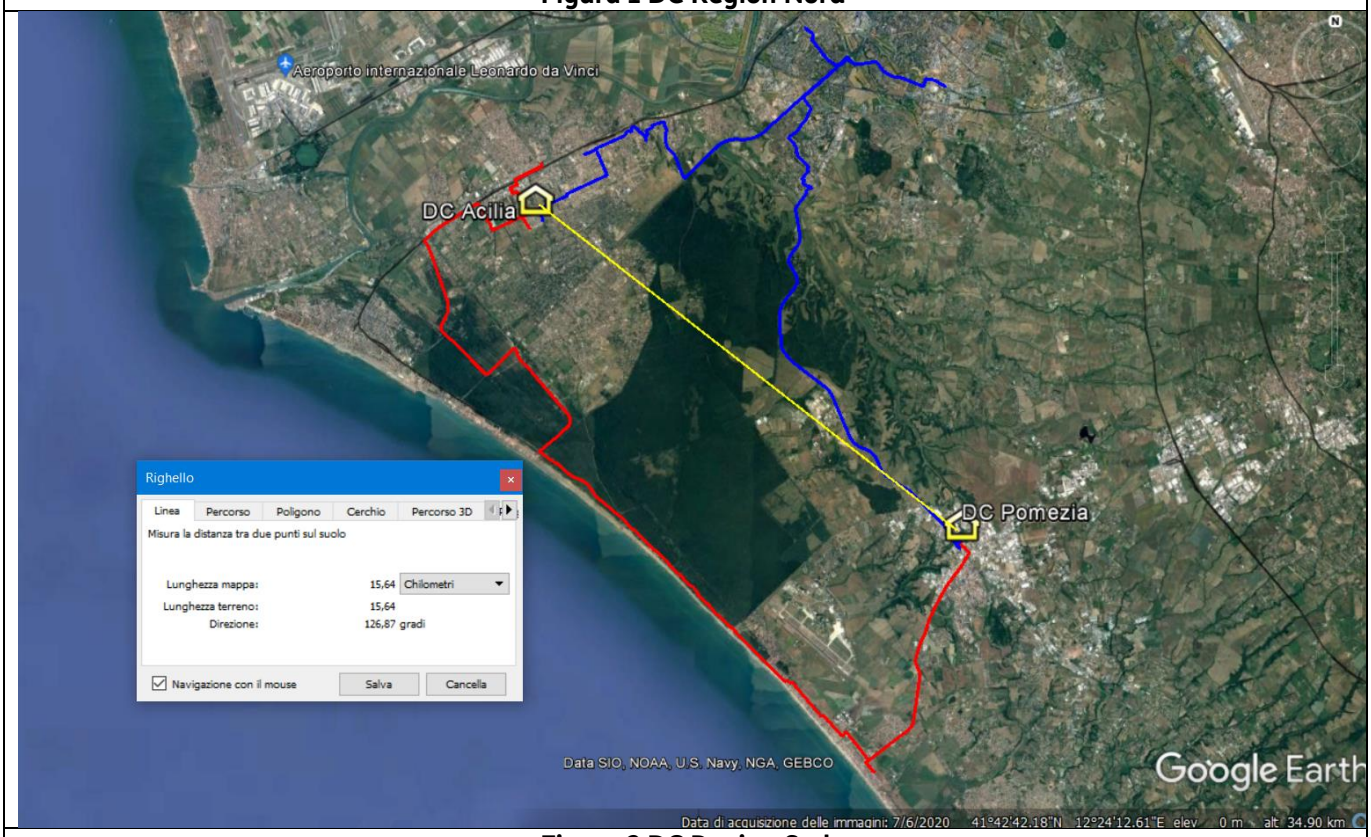



**Figura 2 DC Region Sud**

# 2 Presentazione del costituito RTI

## 2.1 TIM S.p.A.

TIM è una delle principali realtà ICT in Italia. Lavora per un'Italia sempre più digitale, per rispondere alle esigenze dei cittadini, delle imprese e delle istituzioni, anche nei momenti più difficili. Grazie a interventi realizzati su tutto il territorio, intensificati durante l'emergenza sanitaria per permettere al Paese di non fermarsi durante il lockdown, la fibra ottica di TIM ha connesso già a dicembre 2020 il 90% delle famiglie con linea fissa, con l'obiettivo di chiudere il digital divide in Italia entro il 2021, estendendo a tutti la possibilità di lavorare e studiare a distanza, navigare ad alta velocità e usufruire dei servizi TV e d'intrattenimento. Con l'ultrabroadband mobile LTE TIM viene raggiunto oltre il 99% della popolazione, mentre il 5G TIM raggiungerà la copertura nazionale entro il 2025/2026.

Al centro della strategia del Gruppo i clienti, quasi 100 milioni fra Italia e Brasile, a cui viene offerta una connettività convergente e sempre più ricca: insieme alle telecomunicazioni fisse e mobili anche TV, contenuti digitali per l'entertainment - video, musica, gaming - e soluzioni per la casa intelligente.

Numerosi gli investimenti nell'innovazione e nelle nuove frontiere del cloud ed edge computing, per offrire piattaforme e soluzioni innovative per la digitalizzazione delle imprese, dalle PMI alla grande industria, fino al mondo della pubblica amministrazione e della sanità. Diventano così sempre più smart realtà produttive e territori.

Da 18 anni TIM è presente nei principali indici di Sostenibilità, segno dell'impegno e dell'attenzione agli effetti delle proprie attività sulla comunità e sull'ambiente per una crescita sostenibile. Con il progetto Operazione Risorgimento Digitale - la prima grande scuola di Internet gratuita che opera grazie al contributo di 30 partner e con il sostegno di associazioni di categoria, terzo settore e importanti attori nel campo della innovazione sociale – vengono diffuse competenze digitali nel Paese. Un'iniziativa di cui hanno già fruito oltre 700.000 cittadini. E per quanto riguarda il footprint ambientale, l'azienda ha fissato l'obiettivo di diventare carbon neutral entro il 2030.

Il gruppo si avvale di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e pubbliche amministrazioni, anche in partnership con gruppi di primaria importanza: Noovle è la cloud company di TIM, leading cloud enabler e Centro di Eccellenza a supporto della trasformazione digitale delle aziende pubbliche e private italiane; Sparkle, primo fornitore di servizi wholesale internazionali in Italia e fra i primi 10 a livello globale, con una delle più grandi e avanzate reti al mondo; Olivetti è il polo digitale con focus sullo sviluppo di soluzioni Internet of things, Telsy opera nel settore della cybersecurity.

I numeri di TIM al 31 dicembre 2021:

- 30,5 milioni le linee mobili in Italia;
- 16,4 milioni gli accessi totali alla rete fissa;
- 52,1 milioni le linee di TIM Brasil;
- 52.480 il personale, di cui 42.827 in Italia.

## 2.2 CDP Equity S.p.A.

CDP Equity S.p.A. (di seguito anche "CDP Equity" o la "Società"), costituita nel 2011 con il nome Fondo Strategico Italiano S.p.A. e rinominata in CDP Equity nel 2016, è un investitore paziente di lungo periodo e agisce secondo logiche di mercato. Gli interventi in settori strategici, con ritorni adeguati, sono connaturati alla sua missione di sostenere lo sviluppo del Paese. CDP Equity, che è una realtà controllata al 100% dal Gruppo CDP, opera acquisendo prevalentemente quote di minoranza in imprese di rilevante interesse nazionale, che siano in equilibrio economico-finanziario e presentino adeguate prospettive di redditività e sviluppo

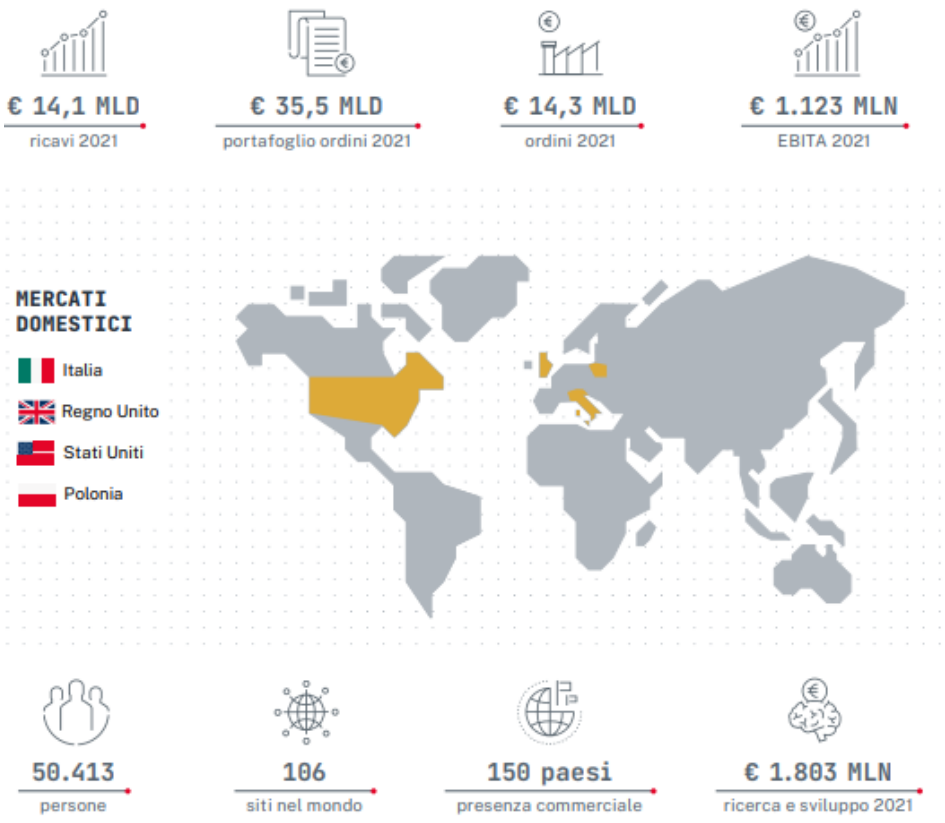
CDP Equity investe in aziende di rilevante interesse nazionale, attraverso partecipazioni dirette e indirette. Mette a disposizione capitali per lo sviluppo a lungo termine di organizzazioni in settori chiave per favorire l'innovazione in tecnologie e infrastrutture indispensabili alla crescita del sistema Paese. Attraverso partecipazioni in fondi, e in fondi di fondi, supporta l'ecosistema imprenditoriale italiano. È inoltre un investitore di riferimento negli asset alternativi. In particolare, CDP Equity, che ad oggi ha investito complessivi 4,9 miliardi di euro, effettua:

- ***Investimenti Diretti*** intervenendo, in base al proprio statuto, in aziende che operano in settori strategici per lo sviluppo del Paese e in grado di generare impatto rilevante sull'economia italiana. Per favorire percorsi di consolidamento, espansione e internazionalizzazione, gli interventi di CDP Equity mirano ad intercettare i più rilevanti mega-trend: dalla transizione energetica alla digital transformation, dall'industria 4.0 al commercio internazionale. Restano al di fuori del perimetro gli investimenti in holding finanziarie di partecipazioni diversificate. Attualmente CDP Equity detiene partecipazioni dirette in 14 società di cui 4 sono società quotate;
- ***Investimenti Indiretti*** agendo come investitore cornerstone in fondi diretti e fondi di fondi gestiti dalle società di asset management di cui è azionista, garantendone la piena autonomia operativa e gestionale. CDP Equity agisce seguendo una rigorosa disciplina di investimento con un processo

che prevede un'attenta attività di negoziazione e due diligence (con particolare attenzione agli aspetti ESG) e gestione dei fondi partecipati. Attualmente CDP Equity detiene partecipazioni in 5 SGR e ha investito in 7 fondi gestiti dalle medesime SGR.

## 2.3 Leonardo S.p.A.

Con oltre 50.000 dipendenti, Leonardo è leader industriale e tecnologico del settore Aerospazio, Difesa e Sicurezza, con un portafoglio bilanciato e geograficamente distribuito e una rilevante presenza industriale in Italia, Regno Unito, Polonia e Stati Uniti. Un approccio sostenibile di business e una strategia finanziaria disciplinata sono i pilastri principali sui quali si basa la creazione di valore per tutti gli stakeholder. L'attenzione alla sostenibilità di Leonardo è testimoniata dai risultati raggiunti sul fronte **ESG**, riconosciuti anche a livello globale, grazie alla presenza del Gruppo in diversi importanti rating, indici e ranking di sostenibilità. Di particolare rilevanza si ricordano: il raggiungimento del punteggio più alto del settore Aerospazio e Difesa nel **Dow Jones Sustainability Index** di S&P Global per il terzo anno consecutivo, il riconoscimento di **UN Global Compact LEAD** per l'impegno all'interno della più grande iniziativa globale sulla sostenibilità d'impresa, l'inclusione nel MIB ESG Index lanciato da Borsa Italiana nel 2021, la conferma nella A list di CDP Climate Change e nel Bloomberg Gender Equality Index. Nel corso del 2021 Leonardo si è confermata partner dell'Italia nel processo di transizione digitale, ecologica e industriale, in linea con quanto previsto nel Piano Strategico **Be Tomorrow - Leonardo 2030**. Il Gruppo, attraverso ogni sua Divisione e Società, ha le competenze utili a intercettare tutte le sei missioni del **PNRR**, coinvolgendo stakeholder privati e pubblici, quali ad esempio i Ministeri della Transizione Digitale, delle Infrastrutture e della Mobilità Sostenibile, della Salute, dell'Università e della Ricerca, dell'Istruzione, della Cultura, della Transizione Ecologica, e quello per il Sud.




Leonardo si presenta sul mercato come un provider globale di sistemi, prodotti e soluzioni all'avanguardia in grado di rispondere alla crescente domanda di tecnologie avanzate nei settori della sicurezza, dell'informatica, della protezione di informazioni, infrastrutture e territorio, nonché nella gestione di infrastrutture strategiche. Con investimenti per 1,8 €mld nel 2021, la collaborazione con 90 Università e centri di ricerca e l'impiego di 9.600 persone, Leonardo è fra le prime in Europa e nel mondo tra le maggiori aziende che investono in Ricerca e Sviluppo nel settore dell'Aerospazio, Difesa e Sicurezza. I processi di innovazione sono supportati da 10 LABS a livello internazionale, di cui 6 in Italia.

Nel settore Sicurezza opera la **Divisione Cyber & Security Solutions** che, sfruttando le sinergie tra information technology, comunicazioni, automazione, sicurezza fisica e digitale, mette a disposizione dei propri clienti know-how, processi e tecnologie avanzate. Tale Divisione realizza piattaforme applicative per l'erogazione di servizi digitali, supportando l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle Agende Digitali Nazionali ed Europee. La Divisione Cyber & Security Solutions vanta infatti pluriennali esperienze maturate presso le principali Amministrazioni Pubbliche Centrali e Locali, risultando negli anni spesso aggiudicataria dei principali Contratti Quadro Consip nell'ambito Infrastrutture e Sicurezza e Applicativi, finalizzati a indirizzare il processo di Digital Transformation, tra cui il Contratto per l'affidamento di servizi in ambito Sistemi Gestionali Integrati per le Pubbliche Amministrazioni – Lotto 1 (2017-2022), la Convenzione SPC Cloud – Lotto 2 (2015-2022) e l'Accordo Quadro System Management 2 (2019-2022), Accordo Quadro Data Management e PMO – Lotto 1, 2 e 3 (2022-2024).

In particolare, vengono offerte soluzioni innovative per l'erogazione di servizi digitali nei seguenti ambiti, svolgendo il ruolo di partner d'eccellenza nel processo di Digital Trasformation:

***Soluzioni di Cybersecurity:*** Grazie al nostro know-how nella protezione di paesi e di infrastrutture nazionali critiche, forniamo soluzioni e servizi che garantiscono il massimo livello di protezione e resilienza, incrementando la capacità di anticipare le minacce, controllare i rischi e gestire efficacemente gli attacchi cyber;

- ***Comunicazioni professionali***: Le nostre reti integrate e piattaforme di comunicazioni sicure sono in grado di soddisfare i più stringenti requisiti di affidabilità, anche in situazioni di emergenza, richiesti da agenzie di pubblica sicurezza, protezione civile e infrastrutture critiche;
- ***Sistemi di gestione e controllo***: Progettiamo e sviluppiamo piattaforme integrate di comando e controllo per la sicurezza urbana, la protezione delle infrastrutture critiche e dei grandi eventi, la gestione delle emergenze e il controllo del territorio;
- ***Sistemi di automazione***: Forniamo sistemi di automazione per la gestione dei bagagli negli aeroporti, basati su tecnologia all'avanguardia cross-belt, e sistemi di smistamento, movimentazione e tracciatura di lettere e pacchi per operatori postali e corrieri;
- ***Soluzioni per mercati***: Offriamo soluzioni innovative chiavi in mano, ritagliate sulle esigenze di sicurezza specifiche di ogni mercato, volte a migliorare la sicurezza dei cittadini e l'efficienza e la resilienza di organizzazioni pubbliche, private e delle infrastrutture critiche.

## 2.4 Sogei S.p.A.

Sogei - Società Generale d'Informatica S.p.A. – è la società di Information Technology, partner tecnologico del Ministero dell'Economia e delle Finanze e interamente partecipata dallo stesso, che opera sulla base del modello organizzativo dell'in-house providing.

Nata nel 1976 come società a partecipazione pubblica, in esecuzione di una specifica previsione normativa, per la realizzazione dell'Anagrafe tributaria, Sogei è oggi la "piattaforma digitale" dell'Amministrazione Finanziaria, che offre soluzioni, competenze e asset, all'interno di un'infrastruttura strategica altamente affidabile.

Ulteriori previsioni normative hanno negli anni esteso negli anni la lista delle pubbliche amministrazioni e istituzioni Clienti, ampliando know-how e competenze e rendendo l'Azienda una risorsa unica del Paese, per efficienza, solidità, sicurezza e alta affidabilità, capace di tradurre le esigenze di innovazione dei propri Clienti in benefici per cittadini, imprese e istituzioni. "Semplifichiamo la vita di Noi cittadini" è il Purpose di Sogei ed è insito nella storia, nell'identità e nella cultura. È ciò che l'Azienda mette al servizio

e che tiene conto delle esigenze e dei bisogni delle persone. Semplificare la fruibilità dei servizi e, quindi, la vita di tutti, supportando la digitalizzazione della PA per un'Italia più moderna e competitiva.

La Società ha 2.210 dipendenti (dati al 31 dicembre 2020) e una partecipazione di minoranza nella società Geoweb, società in controllo pubblico, costituita insieme al Consiglio Nazionale geometri e Geometri Laureati per offrire servizi IT ai professionisti.

Le attività oggetto della gara saranno erogate dalla NewCo che sarà costituita successivamente all'aggiudicazione. TIM S.p.A. (mandataria), Leonardo S.p.A. e Sogei S.p.A (mandanti) partecipano alla NewCo in qualità di soci industriali e partecipano all'esecuzione delle prestazioni oggetto della fornitura erogando servizi direttamente alla NewCo. CDP Equity S.p.A. partecipa alla NewCo in qualità di mandante-investitore istituzionale e non partecipa all'esecuzione delle prestazioni oggetto della fornitura e non eroga servizi direttamente alla NewCo.

## 3 ID 1 – Tabellare - Miglioramento del PUE misurato su base annuale per ciascun anno e per ciascun Data Center a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 1,5

Il costituito RTI in relazione alla premialità relativa al miglioramento dell'efficienza energetica dell'infrastruttura si impegna ad un **miglioramento del PUE**, misurato su base annuale per ciascun anno e per ciascun Data Center a partire dal terzo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto, **per un valore pari o inferiore 1,3** rilevato in prossimità del punto di funzionamento ottimale, 85% del riempimento della sala, come da chiarimento n 1.23 contenuto nelle FAQ 3.

## 4 ID 2 – Tabellare - Miglioramento della % di approvvigionamento elettrico da fonti rinnovabili anche ai fini dell'indipendenza energetica per il relativo approvvigionamento misurato per ciascun Data Center su base annuale per ciascun anno a partire dal secondo anno dalla stipula del contratto e da mantenere per tutti gli anni successivi fino alla scadenza del contratto rispetto al valore base pari a 50%

Il costituito RTI, in relazione alla premialità relativa alla riduzione dell'impatto ambientale, **propone un miglioramento della % di approvvigionamento elettrico** da fonti rinnovabili anche ai fini dell'indipendenza energetica per il relativo approvvigionamento **per un valore superiore al 99% per ciascun Data Center su base annuale** a partire dal secondo anno dalla stipula del contratto per tutti gli anni successivi fino a scadenza contratto.

# 5 ID 3 – Tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di informazioni personali, quali certificazioni della famiglia ISO/IEC 29100 oppure ISO/IEC 27701

Il costituito RTI, in risposta al criterio ID 3, in relazione alla premialità nella gestione di informazioni personali, **conferma la titolarità della certificazione di sicurezza ISO 27701 e la presenza di personale con certificazioni ISO 29100**. Si rimanda all'allegato 01 per le relative certificazioni.

# 6 ID 4 – Tabellare - Titolarità di certificazioni di sicurezza in materia di gestione di incidenti di sicurezza, quali la ISO 27035.

Il Costituito RTI, in relazione alla premialità relativa alla competenza nella gestione di incidenti di sicurezza, **conferma la titolarità delle certificazioni di sicurezza in materia di gestione di incidenti di sicurezza richieste, ossia la ISO/IEC 27035-1 e la ISO/IEC 27035-2**. Si rimanda all'allegato 02 per le relative certificazioni.

# 7 ID 5 – Tabellare - Incremento del numero di fornitori di servizi di public cloud (CSP qualificati) rispetto al valore base della proposta pari a 3 con i quali il concorrente si impegna a far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: Public Cloud PSN Managed, Secure Public Cloud, Hybrid Cloud on PSN Site

Il costituito RTI, in risposta al criterio ID 5, in relazione alla premialità legata all'incremento del numero di fornitori di servizi di public cloud, **si impegna ad incrementare il numero di fornitori di public cloud (CSP qualificati),** rispetto al valore base della proposta pari a 3**,** con cui far stipulare accordi alla NewCo per l'offerta dei servizi in tutti i seguenti ambiti: Public Cloud PSN Managed, Secure Public Cloud, Hybrid Cloud on PSN Site.

# 8 ID 6 – Tabellare - Miglioramento dell'offerta di servizi cloud mediante utilizzo di tecnologia Open Source. Per tali servizi, l'offerta tecnica deve prevedere la descrizione della componente tecnica e la descrizione delle tempistiche di disponibilità di tali servizi che saranno inseriti in sede di aggiornamento del listino prezzi, comunque non oltre i 2 anni dalla sottoscrizione della Convenzione

Il costituito RTI, in risposta al criterio ID 6, in relazione alla premialità legata al miglioramento dell'offerta di servizi mediante utilizzo di tecnologia Open Source, si impegna ad inserire nel listino prezzi ed a rendere disponibili, entro due anni dalla sottoscrizione della Convenzione, in tutti gli ambiti dell'offerta:

- **almeno 1 servizio cloud** basato su tecnologia open source nell'ambito dei **servizi Private Cloud**;
- **almeno 1 servizio cloud** basato su tecnologia open source nell'ambito dei **servizi Public Cloud PSN Managed**;
- **almeno 1 servizio cloud** basato su tecnologia open source nell'ambito di **Secure Public Cloud e Hybrid Cloud on PSN Site**.

Nella seguente tabella si riassumono tutti **i servizi offerti** descritti poi nel dettaglio nei successivi paragrafi dedicati, classificati per ambito di servizi e con l'indicazione delle relative tempistiche di disponibilità a partire dalla sottoscrizione della convenzione:

| Ambito dei servizi | Servizio basato su tecnologia Open Source | Tempo di disponibilità |
|---|---|---|
| Private Cloud | **Servizio 1** - Piattaforma per Container (CaaS) basata su tecnologia Open Source OKD - cfr §8.1 | Entro 22 mesi |
| | **Servizio 2** - Piattaforma per collaboration basata su tecnologia Open Source Mattermost - cfr §8.2 | Entro 22 mesi |
| Public Cloud PSN Managed | **Servizio 1** - Piattaforma per Container (CaaS) basata su tecnologia Open Source OKD - cfr §8.1 | Entro 22 mesi |
| | **Servizio 2** - Piattaforma per collaboration basata su tecnologia Open Source Mattermost - cfr §8.2 | Entro 22 mesi |

| | | |
|---|---|---|
| Secure Public Cloud | **Servizio 1** - Piattaforma per Container (CaaS) basata su tecnologia Open Source OKD - cfr §8.1 | Entro 22 mesi |
| | **Servizio 2** - Piattaforma per collaboration basata su tecnologia Open Source Mattermost - cfr §8.2 | Entro 22 mesi |
| Hybrid Cloud on PSN Site | **Servizio 1** - Piattaforma per Container (CaaS) basata su tecnologia Open Source OKD - cfr §8.1 | Entro 22 mesi |
| | **Servizio 2** - Piattaforma per collaboration basata su tecnologia Open Source Mattermost - cfr §8.2 | Entro 22 mesi |

Nei paragrafi seguenti sono descritte in dettaglio le tecnologie Open Source su cui sono basati i servizi cloud che saranno resi disponibili dal PSN ad incremento dell'offerta. Tali soluzioni garantiscono alle amministrazioni pubbliche italiane la "***Sovranità del Software***", ovvero la possibilità di sviluppare applicazioni che non hanno una stretta dipendenza da tecnologie e/o servizi forniti da uno specifico vendor o provider, rimuovendo così il rischio di *lock-in* tecnologici e commerciali. La scelta di tecnologie Open Source garantisce inoltre la massima compatibilità con le altre tecnologie IT e/o di sicurezza che potranno essere introdotte anche in seguito, facendo propri i principi della portabilità, dell'interoperabilità e della condivisione dei dati richiesta dall'EU Data Act.

## 8.1 Piattaforma per container (CaaS) basata su tecnologia Open Source OKD

- **Ambito di applicabilità:** *tutti gli ambiti di servizi*.

Il servizio proposto va ad incrementare l'offerta del costituito RTI, fornendo una soluzione tecnologica open source applicabile in maniera uniforme su tutti gli ambiti, e specificamente per la classe di servizi dei **container** (CaaS). L'utilizzo dei container si presta in maniera particolarmente efficace a questo scopo, essendo una tecnologia di astrazione delle risorse sia infrastrutturali (hardware fisico o virtuale), sia sistemistiche (hypervisor, sistemi operativi) progettata per un utilizzo flessibile, elastico, multipiattaforma e multi-cloud, adottata anche per la progettazione di applicazioni native per il cloud (*cloud native*). La tecnologia dei container consente inoltre la progettazione di applicazioni con un approccio a micro-servizi, abilitando il rilascio del codice applicativo in modo omogeneo su diverse piattaforme infrastrutturali e sistemistiche, utilizzando solo le risorse necessarie ad eseguire il codice, in maniera segregata e sicura.

Allo stato dell'arte, i container rappresentano anche il modello più sicuro e versatile per il rilascio del codice e l'erogazione dei servizi applicativi, beneficiando dei punti di forza sia dei modelli più tradizionali (installazioni bare metal di sistemi operativi o virtualizzazione dei sistemi tramite hypervisor), sia dei modelli più innovativi (serverless e Function-as-a-Service).

Il servizio offerto si basa sul **progetto Open Source OKD** (https://www.okd.io/), già noto come **OpenShift Origin** (distribuzione community di openshift), una soluzione che nasce dall'evoluzione di **Kubernetes**, noto progetto open source per l'orchestrazione dei container, oggi mantenuto dalla **Cloud Native Computing Foundation (CNCF),** a cui sono aggiunte funzionalità di sicurezza e ottimizzazioni per il deploy in ambiente multi-tenant, progettate specificamente per ambienti di livello "*enterprise*". Il "motore" Kubernetes rimane dunque un componente "*core*" del progetto di community (container cluster management): il vantaggio dell'approccio Open Source è il contributo attivo di una community di partner in continua espansione che, attraverso la proposizione di soluzioni integrative (storage, networking, ISV, integrazioni IDE e CI compatibili con OpenShift Container Platform), rendono il prodotto più versatile ed innovativo. Essendo un servizio basato sull'astrazione dei container, può essere utilizzato su qualsiasi ambiente, per i vari ambiti di servizio previsti nell'offerta. Tutte le funzionalità aggiuntive della piattaforma accelerano la produttività degli sviluppatori, assicurando alle applicazioni la portabilità nel cloud ibrido, grazie al supporto di una community estesa.

In particolare, per l'erogazione del servizio sarà utilizzata la distribuzione Red Hat di OpenShift, di cui OKD è il corrispondente progetto parallelo di community, su cui è basata appunto questa distribuzione: come per tutte le distribuzioni Red Hat, sul portale di accesso (access.redhat.com) è sempre disponibile il relativo codice sorgente, per ogni componente software RPM: il codice è quindi aperto.

La distribuzione Red Hat di OpenShift aggiunge alla corrispondente **distribuzione gemella** di community, su cui si basa, il necessario livello di affidabilità che deriva dalla costante revisione di un team di esperti dedicati, oltre ad ulteriori funzionalità per la produttività e la sicurezza, tra cui registro, reti, telemetria, sicurezza, automazione, anch'essi basati a loro volta su altri progetti open source, che aiutano a sfruttare meglio il potenziale del software di orchestrazione, tra cui:

- Registro - es. *Atomic Registry, Docker Registry*;
- Rete – es. *OpenvSwitch*;
- Telemetria - es. *Heapster, Kibana, Hawkular, Elastic*;
- Sicurezza – es. *LDAP, SELinux, RBAC, OAUTH*;
- Automazione – es. *Ansible*.

In seguito al deployment di cluster e applicazioni, la gestione del ciclo di vita di queste componenti, le console destinate a operatori e sviluppatori e la sicurezza diventano aspetti di fondamentale importanza. Red Hat OpenShift offre installazione, aggiornamenti e gestione del ciclo di vita automatizzati per tutte le componenti dello stack del container: sistema operativo, Kubernetes, servizi e applicazioni del cluster. Ne risulta una piattaforma applicativa Kubernetes più sicura e sempre aggiornata, priva delle complessità tipiche degli aggiornamenti manuali e seriali, e senza interruzioni dell'operatività. La piattaforma si integra con Jenkins e altri strumenti standard di integrazione e deployment continui (CI/CD), nonché con gli strumenti e i flussi di lavoro integrati di OpenShift, per creare applicazioni sicure; integra container OCI/Docker e Kubernetes certificati da Cloud Native Computing Foundation (CNCF) per l'orchestrazione dei container, ed altre tecnologie open source.

Le immagini dei container realizzate con lo **standard Open Container Initiative (OCI)** assicurano la portabilità tra le workstation di sviluppo e gli ambienti di produzione di OpenShift Container Platform.

La piattaforma può essere quindi **utilizzata nei diversi ambiti previsti in modo uniforme**, fornendo sia al gestore che all'utilizzatore un'esperienza coerente, omogenea e replicabile. Questa caratteristica consente una fruizione nei diversi ambiti di servizi proposti dal bando, secondo lo stesso schema di gestione: l'architettura proposta è quindi identica al variare dell'ambito di applicazione; questo è reso possibile dalla portabilità di OpenShift e dagli strumenti automatici di installazione e interfacciamento che astraggono dalle complessità e le specificità implementative.

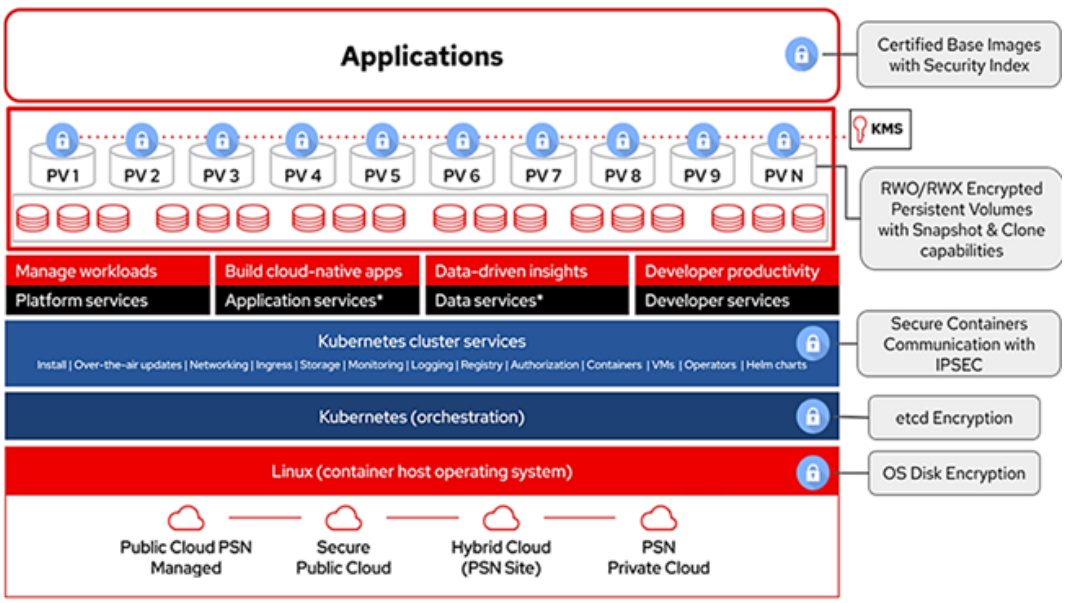



**Figura 3 Architettura OCI**

## Sicurezza

Operando ad un livello di astrazione basato sui container e grazie al continuo supporto della community, Red Hat Openshift è adatto a seguire costanti politiche di aggiornamento che lo rendono una valida soluzione nell'introduzione di nuove features e rimediare a potenziali esposizioni di sicurezza sia software (Advanced Cluster Security for Kubernetes) che attraverso semplici attività di manutenzione ed aggiornamento dell'hardware sottostante.

La gestione delle vulnerabilità, infatti, è costantemente monitorata da due team (Openshift Security Team e Red Hat Security Team) che, mediante l'invio di notifiche, indicano la presenza di aggiornamenti di sicurezza (bugfix).

La **protezione delle applicazioni** containerizzate si basa su **più livelli di sicurezza**:

- immagine base di container affidabile e sicura, attraverso un processo di creazione con pipeline CI/CD;
- capacità di scansionare le immagini dei container per individuare le vulnerabilità, con strumenti efficienti per correggere e sostituire le immagini vulnerabili;
- conservazione sicura dei dati salvati dai container (*at-rest*), rendendo tali dati inaccessibili da applicazioni e utenti non autorizzati;
- comunicazione sicura dei dati (*in-transit*) tra container diversi all'interno della stessa piattaforma di orchestrazione Kubernetes;
- esecuzione su sistemi operativi e reti protette, con definizione di confini netti tra il container stesso e gli utenti e gli host che interagiscono con esso.

Red Hat Openshift supporta il **Multi-Tenancy**, per cui più clienti possono condividere la stessa applicazione, in esecuzione sullo stesso sistema operativo, con lo stesso meccanismo di archiviazione dei dati hosting condiviso. Le risorse server che sono suddivise tra diversi clienti includono un livello di personalizzazione per i tenant, ad esempio la possibilità per il tenant di decidere in merito ad autorizzazioni e restrizioni specifiche di controllo dell'accesso per gli utenti (RBAC).

La segregazione è garantita dall'adozione di meccanismi come:

- *Linux Namespaces* (caratteristica del kernel Linux che suddivide le risorse del kernel in modo tale che un insieme di processi veda solamente un insieme di risorse);
- *SELinux* (strato di sicurezza per isolare i container l'uno dall'altro);

- *CGroups* (Control Groups - funzionalità del kernel Linux che limita, tiene conto ed isola l'utilizzo delle risorse di una collezione di processi).

L'**ambiente di management** (tenant) della soluzione Openshift è naturalmente soggetto agli stessi meccanismi di sicurezza appena elencati per garantire la segregazione con gli ambienti cliente.

Attraverso l'ambiente di management, oltre alla completa gestione dell'architettura, è possibile automatizzare il rilascio degli ambienti cliente con l'applicazione delle relative policy utente.

Red Hat Openshift integra inoltre i più diffusi protocolli di ***Single-Sign-On* (SSO)**:

- SAML (standard usato per autorizzazioni tra service provider ed identity provider);
- OAUTH (autorizzazione ed autenticazione basata su token).

L'integrazione con Red Hat Single Sign-On (software open-source) inoltre assicura che l'accesso logico avvenga attraverso meccanismi aggiuntivi alla password (**Two Factor Authentication**) in linea con le best practice di settore.

Red Hat Openshift riesce ad interfacciarsi con *Luna HSM* e *Luna Cloud HSM* (*Thales HSM*) per la gestione delle chiavi esterne (**Key Management**), utile all'encryption di volumi (container storage), *Object Storage Daemon* (OSD), *Multicloud Object Gateway* (MCG), *Rados Block Device* (RBD): l'encryption è garantita anche in caso di clone o snapshot del volume (*Enhanced Block Device*).

È possibile, inoltre, attivare ulteriori funzionalità di encryption come *etcd data encryption* (cifratura del database interno etcd) e IPsec, che consente ai pod all'interno di un cluster di comunicare tra di loro attraverso un tunnel cifrato.

Un ulteriore elemento per garantire la sicurezza dei dati è l'utilizzo di NBDE (*Network-Bound Disk Encryption*) che consente di crittografare i volumi root dei dischi rigidi su macchine fisiche e virtuali senza dover immettere manualmente una password al riavvio delle macchine. NBDE lega efficacemente la chiave di crittografia a un server esterno o a un insieme di server in modo sicuro e anonimo attraverso la rete: i nodi non hanno così la necessità di memorizzare la chiave di crittografia né trasferirla sulla rete.

Openshift si integra inoltre con i seguenti componenti Open Source per tracciare, raccogliere e archiviare i **log di piattaforma**:

- *Fluentd*, per la collezione dei log e l'inoltro verso un logstore;
- *Elasticsearch*, un logstore che salva e ruota i log in base alle configurazioni definite;
- *Kibana*, interfaccia web che permette la visualizzazione dei log con relativi grafici e statistiche.

Per impostazione predefinita, OpenShift invia i log dei containers e dell'infrastruttura all' Elasticsearch interno ed è possibile ridondare l'archiviazione dei log smistandoli su aggregatori esterni attraverso l'utilizzo dei Log Forwarder (protocolli Fluentd, Syslog oppure OpenShift Container Platform Log Forwarding API). L'invio dei log di container, infrastruttura e audit verso endpoint specifici all'interno o all'esterno del cluster, avviene attraverso protocollo criptato TLS (Transport Layer Security) in modo da garantirne la manomissione, la falsificazione e l'intercettazione.

## 8.2 Piattaforma per collaboration basata su tecnologia Open Source Mattermost

- **Ambito di applicabilità:** *tutti gli ambiti di servizi.*

Mattermost è una piattaforma open source di collaborazione sicura e condivisione di contenuti e costituisce un'alternativa Open Source a prodotti di mercato come MS Teams o Slack: il progetto è reso disponibile su GitHub. Il software, sviluppato in collaborazione con migliaia di sviluppatori da tutto il mondo, è progettato per aumentare l'agilità, l'efficienza e l'innovazione nelle organizzazioni ad alta affidabilità, mantenendo al contempo dati e operazioni sotto il controllo IT. Mattermost è molto diffuso nel settore scientifico/tecnologico e non-profit e può beneficiare di un ricco ecosistema di contributi e personalizzazioni della community.

Mattermost offre una vasta gamma di metodi per aggiungere funzionalità e personalizzare l'esperienza in base alle esigenze, ad esempio per nuove funzionalità utente o creare una chatbot avanzata. Le app sono componenti aggiuntivi leggeri e interattivi che possono essere scritti in qualsiasi linguaggio di programmazione ed eseguiti su qualsiasi servizio di hosting compatibile con HTTP o diversi provider serverless. È possibile interagire con utenti e canali tramite una moderna API REST che soddisfa la specifica OpenAPI.

Le feature di Mattermost comprendono la condivisione di contenuti, l'instant messaging (chat), la gestione delle riunioni, le chiamate audio/video.

La piattaforma Mattermost integra tre strumenti principali che coprono un'ampia gamma di casi d'uso di collaborazione. Ogni strumento si concentra su un flusso di lavoro primario e può essere utilizzato in combinazione senza soluzione di continuità per la collaborazione in tempo reale e per processi e progetti con durate che vanno da giorni a mesi. I tre strumenti chiave sono:

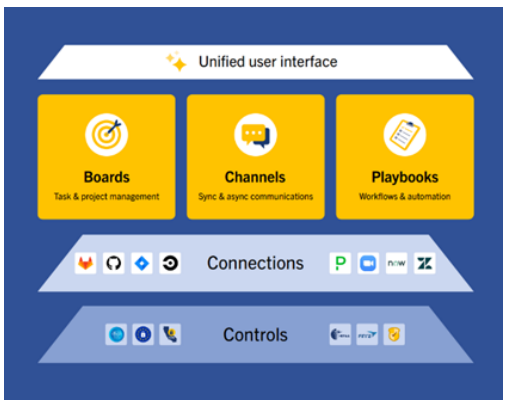



**Figura 4 Strumenti chiave Mattermost**

- Canali - per instaurare un canale di comunicazione con il team e messaggi di gruppo;
- Playbook - processi ripetibili per ottenere risultati specifici e prevedibili;
- Bacheche - organizzazione di progetti e attività in una struttura di bacheca Kanban.

Sono disponibili client desktop per Windows, MacOS e Linux e app mobili per iOS e Android.

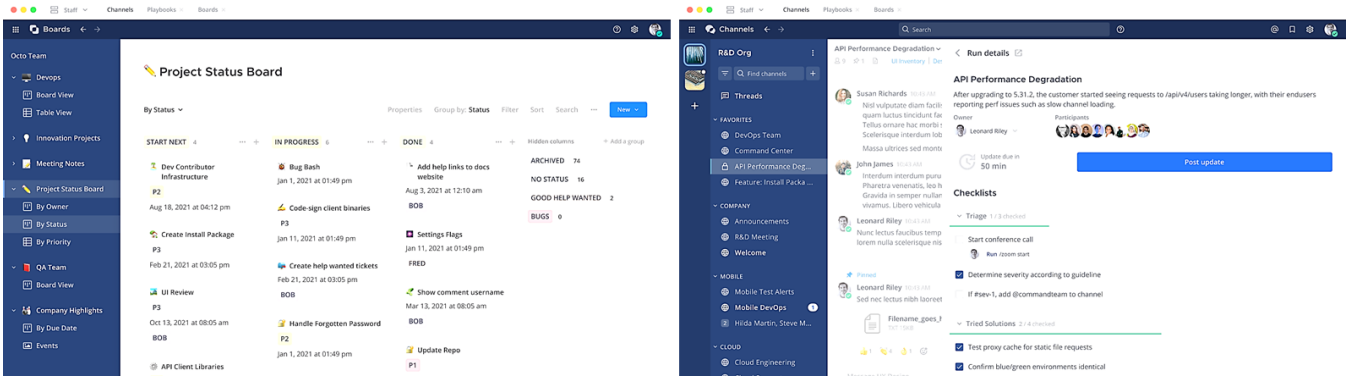



**Figura 5 Esempi interfaccia utente**

Mattermost può essere installato anche in un cloud privato e quindi è perfettamente calabile anche nel contesto del Private Cloud del PSN. In generale quindi, la piattaforma è utilizzabile in maniera uniforme in tutti gli ambiti di servizio previsti.

In particolare, la soluzione consente di implementare logiche di ChatOps sicura perché si poggia su un cluster Kubernetes che consente il controllo completo sui dati in modo da poter soddisfare i più severi requisiti di sicurezza, privacy e conformità. L'integrazione con le principali soluzioni di sicurezza aziendale consente alle Pubbliche Amministrazioni di ottenere un vantaggio strategico bilanciando la conformità e la garanzia del servizio con la velocità di esecuzione.

Le Pubbliche amministrazioni possono quindi evolvere le loro necessità utilizzando la piattaforma per diversi scenari operativi:

- **DevOps:** il tool consente di tenere traccia della roadmap degli sviluppi, pianifica le funzionalità e assegna le attività di sprint con facilità e flessibilità. Consente un approccio di codifica sociale in ottica di rivedere rapidamente le funzionalità richieste con le integrazioni dei repository, ed ottiene input da gruppi e crea una comunità di test per migliorare la qualità del codice. Consente di rilasciare in tutta sicurezza e in tempo con liste di controllo dei processi, monitoraggio CI/CD e automazione;
- **orchestrazione del flusso di lavoro:** le operazioni digitali semplificano la comunicazione, la visibilità e il controllo tra team, processi e strumenti. I flussi di lavoro frammentati diminuiscono

la produttività mentre la soluzione proposta consente la collaborazione in tempo reale fino alla pianificazione a lungo termine perché diversi flussi di lavoro coprono più intervalli di tempo;

- **risoluzione degli incidenti:** quando si eseguono fasi di recovery dovute ad incident di sicurezza la prontezza della risposta è fondamentale, la macchinosità della condivisione delle informazioni, dovuta ad esempio alla presenza di silos, o a carenze nei processi di comunicazione può aumentare i tempi di rientro e lasciare la Pubblica Amministrazione a rischio. Mattermost è una piattaforma di collaborazione in team appositamente progettata per una risposta rapida agli incidenti, con playbook personalizzabili progettati per aiutare il team di sicurezza ad automatizzare la risposta agli incidenti;
- **CI/CD** Collaborare su migliaia o milioni di righe di codice richiede uno stretto allineamento e coordinamento tra team e strumenti. Mattermost garantisce visibilità e controllo sull'intera pipeline CI/CD con la collaborazione basata sul canale, le integrazioni degli strumenti con comunicazione bidirezionale, l'automazione e i bot per ridurre le attività manuali. In questo modo è più semplice documentare le best practice e fornire ai team dei playbook basati su liste di controllo e in modo da centralizzare e automatizzare le notifiche in tutta la toolchain;
- **i team di test e QA Testing** che supportano team di sviluppo di grandi dimensioni e in rapida evoluzione sono sempre ridotti. La soluzione accelera e semplifica il QA con una piattaforma di collaborazione per mantenere QA e dev agili e allineati durante l'intero ciclo di sviluppo riunendo gli strumenti di test, il team e i flussi di lavoro in un unico ambiente;
- **i team IT di IT Service Desk** gestiscono grandi volumi di richieste ogni giorno ma, mentre gli strumenti di IT service Desk hanno funzioni ottime per il ticketing e il monitoraggio, non sono sempre efficaci come supporto per la collaborazione del team. Con così tanti processi manuali, strumenti disparati e comunicazioni che viaggiano su canali come e-mail, testo e telefono, i problemi possono non essere risolti e ripresentarsi facilmente. Mattermost riunisce tutte le esigenze di collaborazione IT in un'unica piattaforma;
- **APM e NPM** Il monitoraggio dell'integrità e delle prestazioni degli ambienti cloud porta ad ottenere una visibilità delle prestazioni ma non consente la creazione di war room per risolvere le problematiche. Mattermost consente alle pubbliche amministrazioni di risolvere i problemi più rapidamente con una soluzione di collaborazione che si integra profondamente con gli strumenti APM e NPM.

L'esecuzione di Mattermost in Kubernetes richiede risorse diverse in base al numero totale di utenti consentendo alla piattaforma di scalare in maniera semplice e dinamica, in tutti gli ambiti di servizio previsti.

## 9 ID 7 – Tabellare - Miglioramento del valore soglia dell'indicatore di qualità IQ04 pari a numero 5 rilievi

Il costituito RTI, in relazione alla premialità per il miglioramento del valore soglia dell'indicatore di qualità IQ04, propone **un valore pari a 0 rilievi.**

## 10 ID 8 – Tabellare - Miglioramento dei seguenti valori: - RTO atteso dell'indicatore di qualità IQ11 pari a 30 minuti - RPO target dell'indicatore di qualità IQ12 pari a 1 minuto - RTO su diversa Region atteso dell'indicatore di qualità IQ13 pari a 4 ore - RPO su diversa Region target dell'indicatore di qualità IQ14 pari a 30 minuti

Il costituito RTI, in relazione alla premialità per il miglioramento degli indicatori di qualità IQ11, IQ12, IQ13 e IQ14, propone i valori di seguito indicati:

- RTO atteso dell'indicatore di qualità IQ11 pari a 10 minuti;
- RPO atteso dell'indicatore di qualità IQ12 pari a 30 secondi;
- RTO atteso dell'indicatore di qualità IQ13 (su diversa Region) atteso pari a 30 minuti;
- RPO atteso dell'indicatore di qualità IQ14 (su diversa Region) target pari a 15 minuti.

## 11 ID 9 – Tabellare - Miglioramento dei valori soglia dell'indicatore di qualità IQ017 con riferimento ai tempi massimi di risoluzione in ore (Priorità 1 <= 4 ore; Priorità 2 <= 8 ore; Priorità 3 <= 12 ore

Il costituito RTI, in relazione alla premialità per il miglioramento dei valori soglia dell'indicatore di qualità IQ017 con riferimento ai tempi massimi di risoluzione in ore propone valori pari a:

- priorità 1 <= 2 ore;

- priorità 2 <= 4 ore;
- priorità 3 <= 6 ore.

## 12 ID 10 – Tabellare - Riduzione sul periodo minimo di disponibilità dell'infrastruttura di 180 giorni. Il cronoprogramma dovrà evidenziare tutti gli step relativi alla disponibilità dell'infrastruttura evidenziando le proposte che presentino la maggior celerità realizzativa

Il costituito RTI, in relazione alla premialità per il miglioramento relativo al periodo minimo di **disponibilità dell'infrastruttura** si impegna a rendere disponibile la stessa **in 120 giorni** come da Gantt allegato (cfr. allegato 03).

## 13 ID 11 – Tabellare - Possesso, in capo al concorrente singolo o associato, della certificazione di responsabilità sociale ed etica SA 8000 o equivalente

La norma SA8000 rappresenta lo standard internazionale che indica i criteri da seguire per certificare il Sistema di Gestione anche nei confronti della responsabilità sociale ed è la prova che l'Azienda si comporta in modo responsabile anche in materia di etica sociale rispettando i requisiti facenti riferimento ai diritti fondamentali dell'uomo e dei lavoratori: • Considerazione per la salute e la sicurezza sul lavoro; • Rifiuto del lavoro obbligato; • Rifiuto del lavoro minorile; • Garanzia per la libertà di associazione.

Il Gruppo TIM è presente nei principali indici e rating di sostenibilità (ESG). L'inclusione in indici e rating ESG è la conferma – effettuata da enti terzi indipendenti riconosciuti sul mercato finanziario - del rispetto, tramite policy, procedure e piani attuativi concreti, misurati anno dopo anno, delle best practice sui temi Sociali, Ambientali (Environmental) e di Governance (ESG):

- **per il 18° anno consecutivo nel Dow Jones Sustainability Index (DJSI)** Europe e World, ottenendo la bronze class per il 2022, unica azienda italiana del settore TLC ad ottenere tale risultato: di 7.500 aziende valutate, il prestigioso riconoscimento viene assegnato alle 700 società con il miglior punteggio (tra l'5% e il 10% del settore top-performance),

- **nell'indice Diversity and Inclusion di Refinitiv (TIM è tra le prime 100 aziende a livello mondiale, top 3 in Italia e nel settore TLC mondiale**) a conferma dell'impegno del Gruppo per le pari opportunità, la non discriminazione, l'inclusione, la valorizzazione e tutela del personale,
- per il secondo anno nel **Bloomberg Gender Equality Index (GEI)**, indice internazionale che traccia le performance di aziende quotate e impegnate sui temi della parità di genere sulla base delle relative politiche di sviluppo, rappresentanza e trasparenza,
- da ultimo, in termini di tempo, nel nuovo **indice MIB® ESG** lanciato da Euronext e **Borsa Italiana**. Il nuovo paniere è dedicato alle aziende Blue Chip quotate in Italia che adottano le migliori pratiche in ambito sociale, ambientale e di governance.

Le informazioni sull'inclusione in indici e rating sono disponibili pubblicamente qui: https://www.gruppotim.it/it/investitori/finanza-sostenibile/indici-rating-ESG.html

Per il 2021 il Gruppo ha redatto il 25° Bilancio consolidato di Sostenibilità (https://www.gruppotim.it/it/investitori/report-presentazioni/report-sostenibilita/report-lettera-stakeholder.html), in linea con la **Advanced COP** (Communication On Progress) https://www.unglobalcompact.org/participation/report/cop/create-and-submit/advanced/455129 che beneficia del forte impegno sui temi sociali, come testimoniato dalla Policy di Gruppo per il rispetto dei Diritti Umani del Gruppo, redatta nel 2015, e i corsi di formazione per i dipendenti, disponibili anche sul web. https://www.gruppotim.it/it/investitori/report-presentazioni/report-sostenibilita/approfondimenti/diritti-umani.html.

TIM è inoltre in possesso delle certificazioni:

- **UNI ISO 45001:2018** Sistemi di gestione per la salute e sicurezza sul lavoro
- **UNI ISO 37001:2016** Sistemi di gestione per la prevenzione della corruzione

Ne consegue che è possibile affermare che TIM rispetta le linee guida di Social Accountability alla base della certificazione SA 8000 testimoniato, oltre che dall'inclusione negli indici sopra riportati, dalla sottoscrizione dei principi del Global Compact fin dal 2002.

Leonardo rispetta le linee guida di Social Accountability alla base della certificazione SA 8000, come testimoniato dalle seguenti certificazioni ed attestazioni:

- Leonardo è stata riconosciuta, per il **secondo anno consecutivo**, **Global Compact LEAD dell'ONU**, attestandosi come **unica tra le principali aziende globali** del settore Aerospazio e

Difesa ad essere inserita nel ristretto gruppo di aziende - complessivamente 37 (di cui quest'anno quattro italiane) - che si distinguono per l'impegno nella promozione dei **Dieci Principi del Global Compact** e nel contributo al raggiungimento dei **Sustainable Development Goals (SDGs)** dell'Agenda ONU 2030. Leonardo è stata nominata "**Global Compact LEAD**" per aver dimostrato il suo costante impegno verso il Global Compact dell'ONU e i suoi Dieci Principi per un business responsabile. Nel 2021, Leonardo ha mostrato il suo impegno per il Global Compact e i Dieci Principi partecipando alla Action Platform su Pace, Giustizia e Istituzioni Forti, e a quella su Finanza Sostenibile (CFO Taskforce) e presentando una **Advanced COP** (Communication On Progress) che indirizza in particolare i principi ed obiettivi in materia **di DIRITTI UMANI, DIRITTI SUL LAVORO, AMBIENTE, ANTI-CORRUZIONE** **https://www.unglobalcompact.org/participation/report/cop/create-and-submit/advanced/458660**.

- Possesso della certificazione **UNI ISO 45001:2018** Sistemi di gestione per la salute e sicurezza sul lavoro
- Possesso della certificazione **UNI ISO 37001:2016** Sistemi di gestione per la prevenzione della corruzione

Si dichiara pertanto che Leonardo soddisfa il criterio, avendo certificazioni ed attestazioni internazionali complessivamente EQUIVALENTI alla SA 8000.

Per le certificazioni si rimanda all'allegato 04.

## 14 ID 12 – Tabellare - Impiego o assunzione di persone con disabilità in quota eccedente l'obbligo minimo di legge, nell'organico della società di progetto (NewCo)

Il costituito RTI, in relazione alle premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31.12.2021, **dichiara l'impiego o assunzione di persone con disabilità in una quota pari a 12 unità** eccedente l'obbligo minimo di legge nell'organico della società di progetto (NewCo).

## 15 ID 13 – Tabellare - Componente lavoro femminile superiore al 10% dell'organico della società di progetto (NewCo)

Il costituito RTI, in relazione alle premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31/12/2021, dichiara una **componente di lavoro femminile superiore al 30%** dell'organico della società di progetto (NewCo).

## 16 ID 14 – Tabellare - Componente lavoro giovanile (età inferiore a 36 anni) superiore al 5% dell'organico della società di progetto (NewCo)

Il costituito RTI, in relazione alle premialità connesse all'applicazione delle Linee Guida per favorire le pari opportunità di genere e generazionali, nonché l'inclusione lavorativa di persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, pubblicate sulla GURI n. 309 del 31/12/2021, **dichiara una componente di lavoro giovanile (età inferiore a 36 anni) superiore al 20%** dell'organico della società di progetto (NewCo).

# 17 ID 15 – Valutativo - Efficacia delle modalità di verifica proposte dal Concessionario, messe a disposizione del concedente, per il rispetto delle seguenti norme e standard europei in materia ambientale (Do no significant harm): - ISO 50001, monitoraggio del PUE, EN 50600, ISO 14064, ISO 14001 e SWD(2020) 55 final); - Indipendenza energetica e fonti rinnovabili; - Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE); - Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva; - Le procedure di approvvigionamento includeranno la gestione dei beni alla fine del loro ciclo di vita, per ridurre al minimo gli sprechi e favorire il riutilizzo e il riciclo dei materiali; - Al termine del ciclo di vita, l'apparecchiatura sarà predisposta per il riutilizzo, il recupero, il riciclaggio e il corretto trattamento in conformità all'allegato VII della direttiva 2012/19/UE.

## 17.1 Executive Summary

Il costituito RTI, in relazione alla premialità relativa alla modalità di verifica del rispetto delle norme ambientali, si impegna a proporre efficaci modalità di verifica del soddisfacimento delle norme e degli standard europei in materia ambientale.

Il documento segue un'analisi delle norme ambientali suddivisa per paragrafi specifici. Per ogni norma ambientale viene fatta una prima analisi e sono indicate le metodologie e gli strumenti intesi come migliorativi ai fini delle verifiche richieste.

Tali metodologie e strumenti, aggiuntivi rispetto le procedure standard di verifica del soddisfacimento e mantenimento delle certificazioni indicate nel criterio, insistono sui seguenti punti di valore:

- disponibilità in qualunque momento dell'anno, da parte della NewCo, per l'espletamento di audit annuali condotti dal Concedente sui processi caratterizzanti la specifica norma in esame. La volontà da parte del Concedente di organizzare l'audit dovrà avere un preavviso di almeno 30 giorni per poter permettere l'organizzazione dell'attività stessa;

- invito di un referente del Concedente a partecipare, una volta l'anno, agli audit interni dediti alla verifica e avanzamento del processo di controllo;
- condivisione con il Concedente di reportistica periodica (report, GANNT di avanzamento verifiche periodiche, ulteriore documentazione esistente da concordare) con frequenza e contenuti specifici variabili a seconda della norma.

Il processo di verifica del rispetto delle norme riportate nel criterio ID 15, verrà svolto dalle funzioni di staff Facility Management e ESG Performance Management, come descritto nel capitolo riferito al criterio ID 17 *Miglioramenti sugli aspetti di governance* cfr. §19. Nell'iter di verifica potrà, inoltre, partecipare il Comitato di Controllo (CdC), a favore del corretto e pubblico monitoraggio del quadro normativo in materia.

## 17.2 ISO 50001

La strategia introdotta dalla NewCo al fine di massimizzare l'efficacia delle modalità di verifica del rispetto di quanto richiesto dalla ISO 50001 è articolata su tre pillar:

1. certificazione di tutti i Data Center da cui saranno erogati i servizi relativi al PSN, in ambito dei servizi Industry Standard;
2. implementazione di uno specifico processo di audit, al fine di permettere il controllo da parte del Concedente del rispetto delle relative norme e prescrizioni;
3. messa a disposizione del Concedente di report e strumenti atti a verificare il raggiungimento degli obiettivi di efficientamento energetico richiesto da tale norma.

In relazione al primo pillar, che permetterà di razionalizzare metodologie e tempistiche di verifica da parte del Concedente, il processo di certificazione dei Data Center proposti sarà concluso **entro il 2022**. Tale certificazione permetterà inoltre di rispondere a quanto richiesto dal criterio **RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore**, indicato nell'allegato dalla **determina n.307/2022** emessa dall' **Agenzia per la cybersicurezza nazionale**

In relazione al secondo pillar, al fine di evidenziare il rispetto di tale norma, i risultati e certificati saranno condivisi con il Concedente, il quale potrà effettuare audit di verifica di quanto previsto dalla relativa normativa.

Tale audit sarà effettuato su richiesta con preavviso di un mese dal CdC ed eventualmente accompagnato da un rappresentante dell'AgID.

Si evidenzia come, applicando il meccanismo di controllo del doppio cieco, sarà possibile, **con frequenza annuale**, eseguire da parte del Concedente, un audit autonomo non pianificato. Nel caso emergessero a valle di tale processo di audit delle non conformità, la NewCo provvederà a sanarle entro le tempistiche indicate dalla normativa ISO 50001.

In relazione al terzo pillar, la NewCo metterà a disposizione del Concedente, una serie di strumenti e report atti a certificare l'effettivo raggiungimento degli obiettivi energetici. A titolo esemplificativo, dato che tali strumenti potranno essere ampliati e arricchiti a seguito dei risultati degli audit e dell'evoluzione tecnologica del PSN, questi potranno essere:

- le aree di "Collaborazione e Monitoraggio" del portale della fornitura, che raccogliendo i dati provenienti dai sistemi BMS (Building Management System) permetteranno al Concedente di avere una vista sui consumi elettrici dell'intero Data Center;
- report condivisi con **frequenza semestrale** che conterranno, tra le informazioni presenti, i trend storici relativi a:
    - baseline energetica;
    - indici EnPA e IPE;
    - raggiungimento degli obiettivi target.

## 17.3 PUE

In relazione alla definizione di PUE, la NewCo si atterrà a quanto previsto nella **Determinazione AgID n. 628/2021 del 15 dicembre 2021** - Adozione del *"Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione*" - e confermato nell'allegato dalla **determina n.307/2022 emessa dall' Agenzia per la cybersicurezza nazionale** in cui il PUE *mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianto ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura del DC e quella sostenuta dagli apparati.*

Di conseguenza, la NewCo, al fine di massimizzare l'efficacia delle modalità di verifica di tale parametro condividerà mensilmente con il Concedente, i report di spesa e il relativo calcolo del PUE, evidenziando al contempo la sua tendenza storica. A titolo esemplificativo, il valore del PUE sarà calcolato secondo la specifica del "The Green Grid",



che detta le linee guida internazionali per il calcolo del PUE. Il PUE sarà quindi calcolato secondo i parametri definiti nella specifica "**WP49-PUE | PUE™: A COMPREHENSIVE EXAMINATION OF THE METRIC**" secondo la seguente formula:

$$PUE = \frac{Total\ Facility\ Energy}{IT\ Energy}$$

La ***Total Facility Energy*** è definita come l'energia spesa, quindi consumata, dedicata esclusivamente al corretto funzionamento dell'infrastruttura del Data Center (impianti di climatizzazione, impianti ausiliari, impianti ausiliari di sala, impianti di riserva) e comprende anche la componente di energia consumata degli apparati IT.

L'***IT Energy*** è l'energia spesa, dall'apparecchiatura IT, ed è definita come l'energia consumata dall'apparecchiatura utilizzata per gestire, elaborare, archiviare o instradare i dati all'interno del server IT.

I valori del PUE saranno forniti al Concedente con misurazione di almeno Livello 1 (L1), come da specifica "**WP49-PUE | PUE™: A COMPREHENSIVE EXAMINATION OF THE METRIC**".

La misurazione di Livello 1 prevede la registrazione almeno mensile del PUE di sala e la sua storicizzazione.

Si rende noto al Concedente che il PUE è direttamente correlato al parametro dinamico dell'energia IT, che in funzione della percentuale di riempimento di sala determinerà i range di PUE minimi e massimi.

Il riempimento di sala è definito come segue:

$$[1] \quad \%DHU = \frac{IT\ Power\ misurata\ [kW]}{IT\ \text{Power}\ massima\ [kW]}$$

***%DHU*** è la percentuale di Data Hall Utilization, definita dal rapporto tra l'***IT Power misurata*** che corrisponde alla potenza IT effettivamente impegnata dagli apparati all'interno della sala e l'***IT Power massima*** che è la massima potenza IT per la quale la sala è progettata. In generale, "The Green Grid" prevede, quale corretto punto di caduta per la misurazione ottimale del PUE una percentuale di riempimento pari al 85%.

Inoltre, il PUE sarà attualizzato ogni anno alle condizioni climatiche esterne considerando i gradi giorno di raffrescamento mensili del sito del Data Center rispetto al primo anno di esercizio in ragione del

rispetto del target minimo a prescindere dalle condizioni climatiche esterne. Per maggiori dettagli si veda https://www.degreedays.net/introduction.

## 17.4 EN 50600

I Data Center che ospiteranno i servizi del PSN sono certificati **ANSI/TIA 942 Rating 4/Rating 3**, anch'essa riguardante le specifiche per la costruzione e l'esercizio di Data Center, di cui esiste un consolidato meccanismo di accreditamento, le cui specifiche sono più vincolanti e restrittive di quanto previsto dalle norme DIN EN 50600.

In aggiunta, la NewCo si impegna ad avviare l'iter di certificazione ISO/IEC TS 22237 (che ha integrato lo standard EN 50600), con l'obiettivo di conseguirla entro l'anno 2023.

La NewCo, oltre a condividere con il Concedente i certificati ufficiali, si rende disponibile per l'espletamento di **audit annuali** condotti dal Concedente sui processi in ambito di certificazione (previo preavviso di almeno 30 giorni) e la fornitura di reportistica periodica (con frequenza e contenuti da concordare).

Si riportano i report periodici che la NewCo si impegna a fornire nella tabella che segue.

*Tabella 1 Illustrazione report periodici*

| REPORT | PARAMETRI |
|---|---|
| Accessi fisici alle data hall che ospitano i sistemi IT del Concedente | Transiti registrati tramite lettori di badge posizionati in corrispondenza dei varchi di accesso |
| Parametri ambientali rilevati nelle data hall che ospitano i sistemi IT del Concedente, in funzione dei dati disponibili sui sistemi di gestione e monitoraggio degli impianti tecnologici (BMS, Building Management System) | Temperatura e umidità |
| Misure elettriche relative alle data hall che ospitano i sistemi IT del Concedente, in funzione dei dati disponibili sui sistemi di gestione e monitoraggio degli impianti tecnologici (BMS, Building Management System). | Potenza, Energia, Calcolo PUE,etc. |

## 17.5 ISO 14064

La NewCo si impegna nell'implementazione di una corretta e credibile strategia di riduzione del proprio impatto climatico nell'erogare i servizi richiesti dal PSN. A tal fine, si impegnerà nel contrastare i cambiamenti climatici con azioni specifiche sintetizzate in un "Bilancio di sostenibilità" che verrà emesso ogni anno e condiviso con il Concedente, nell'ottica di incrementare l'efficacia delle modalità di verifica, in cui:

- saranno evidenziati i trend di riduzione delle emissioni dirette e indirette di gas serra;
- sarà fornita comunicazione periodica delle loro emissioni;
- avranno visibilità le azioni di diffusione della cultura a sostegno delle azioni atte a contribuire alla diminuzione delle emissioni.

Inoltre, sarà adottata una specifica policy interna, condivisa con il Concedente, in cui la NewCo si impegna a contribuire per quanto di propria competenza alla lotta contro i cambiamenti climatici, favorendo così il raggiungimento degli obiettivi definiti a livello nazionale e internazionale. L'obbiettivo della NewCo è quello di raggiungere la carbon neutrality entro il 2030 (emissioni da Scope 1 e 2 – due delle tre macro-classi delle fonti emissive definite dal Greenhouse Gas Protocol (GHG)). Si pone inoltre l'ulteriore obiettivo di raggiungere Net Zero entro la scadenza della Convenzione (tipologia emissioni: Scope 1, 2 e 3). Per traguardare queste mete si realizzeranno una serie di azioni che andranno a incidere sui diversi tipi di emissioni di anidride carbonica, sia quelle prodotte direttamente (Scope1) che quelle generate indirettamente dai consumi di energia elettrica (Scope 2) sia quelle collegate alla propria supply chain (Scope 3). La NewCo, nel corso di tale percorso, ha previsto di approvvigionarsi al 100% di energia elettrica da fonti rinnovabili al fine di azzerare le emissioni di CO2 correlate.



Carbon Footprint Calculator

Al fine di assicurare l'adeguamento e il rilascio delle certificazioni richieste dalla UE in tema di riduzione dell'impatto ambientale nel settore delle TLC (con particolare riferimento alla ISO 14064, che il costituito RTI si impegna ad ottenere entro un termine massimo di 6 (sei) mesi dall'aggiudicazione del Contratto) la NewCo prevede la messa a disposizione del tool Carbon Footprint Calculator (CC).

Il CC sarà uno strumento che permetterà di:

1. offrire un **supporto strumentale e qualitativo** al ruolo del Direttore del Servizio, per effettuare attività di upselling/miglioramento strategico/centralizzazione di servizi offerti dalla NewCo;
2. **creare un ecosistema di servizi agevolati in ottica "green"**, migliorandone prodotti e servizi, calcolandone l'"impronta di carbonio" e le relative strategie di mercato per adeguarsi ai requisiti del Protocollo di Kyoto;

3. **conoscere lo stato di attività in termini di emissioni**, non solo dei prodotti e servizi venduti alle Amministrazioni Aderenti, ma anche del portale della fornitura che delinea il processo di delivery dell'organizzazione (dai workload, fino ai servizi di gestione);
4. il CC sarà i**l volàno per agevolare la NewCo nell'adeguamento e rilascio delle certificazioni richieste dalla UE** (Il calcolo della quantificazione della CFP viene ad oggi effettuato seguendo i requisiti contenuti nella specifica tecnica PAS 2050, emessa dall'ente di normazione britannico BSI, o lo standard emesso dal WRI/WBCSD. Nel 2013 è stata realizzata la pubblicazione del nuovo riferimento normativo univoco a livello internazionale: la specifica tecnica ISO/TS 14067, a cui si aggiunge lo standard di riferimento ISO 14064).

Tutti gli indicatori che verranno forniti dal sistema saranno certificati intendendo con questo che:

- il modello di calcolo degli stessi sarà esplicitato e validato da un ente terzo;
- sarà garantito e certificato il flusso di input di dati misurati da cui si ricavano gli indicatori – o in alternativa i dati statistici utilizzati per il calcolo devono provenire da fonti ufficiali (es. ISTAT).

Dato che presumibilmente, nei prossimi anni, le autorità regolatorie e governative a livello italiano e internazionale definiranno un set di KPI standard, normative da rispettare e certificazioni da ottenere, il Carbon Calculator sarà regolarmente aggiornato per il supporto delle stesse, al fine di garantire i livelli di performance richiesti nell'ambito del rispetto delle normative *green*. Ad oggi i riferimenti maggiormente significativi restano GHG Protocol & ISO 14064-1.

A titolo esemplificativo e non esaustivo, i KPI/indicatori che saranno prodotti dallo strumento:

- per singola architettura cliente per offerta (es: Amministrazione aderente X che ha contrattualizzato offerta Y);
- per singola Amministrazione aderente, raggruppando tutte le offerte sottoscritte;
- per singola architettura per offerta, secondo simulazione;
- raggruppamento per offerta commerciale;
- raggruppamento per gruppo di offerte (ad oggi: Industry Standard, Hybrid Cloud on PSN Site, Secure Public cloud, Public Cloud PSN Managed);
- complessivo totale per tutti gli elementi in ambito.

## KPI FONTI DATI PER CALCOLO PARAMETRI

Indicativamente, il sistema riceverà dati da:

- ERP e sistemi dipartimentali;

- sistemi di monitoraggio delle offerte e piattaforme NewCo;
- sensoristica disponibile;
- database e altre sorgenti.

## KPI GENERALI LEGATI AL MODELLO ESG

Per tutte i servizi Industry Standard saranno disponibili i seguenti indicatori:

| Indicatore | Descrizione |
|---|---|
| PUE DC NewCo | Come indicato nel criterio ID 1 |
| Riduzione delle emissioni GHG | Kg CO2 eq/anno |

## KPI DA PRODURRE PER TUTTE LE OFFERTE

Per tutte le offerte saranno disponibili i seguenti indicatori

| Indicatore | Descrizione |
|---|---|
| Consumi energetici associati | espresso in KW /anno |
| Risparmio energetico grazie alla maggior efficienza NewCo | espresso in KW/anno |
| Riduzione delle emissioni GHG | Kg CO2 eq/anno |

## KPI DA PRODURRE PER LE OFFERTE CLOUD

| Indicatore | Descrizione |
|---|---|
| Consumo energetico associato | In KW/anno |
| Risparmio energetico grazie alla maggior efficienza | in KW/TB/anno (per componenti storage), in KW/GHZ/anno (potenza computazionale) |

| | |
|---|---|
| Risparmio energetico grazie alla maggior efficienza | in KW/TB/anno (per storage), in KW/GHZ/anno (potenza computazionale) |
| Riduzione delle emissioni GHG | Kg CO2 eq/anno |

## KPI DA PRODURRE PER LE OFFERTE DI HOUSING/HOSTING/COLOCATION

| Indicatore | Descrizione |
|---|---|
| Consumo energetico associato | KW/anno |
| Risparmio energetico grazie alla maggior efficienza | espresso in KW /anno, per offerta, cliente, rack |
| Riduzione delle emissioni GHG | Kg CO2 eq/anno |
| Risparmio da utilizzo infrastrutture condivise (networking, security, VAS, ...) rispetto a soluzioni dedicate | espresso in KW /anno |
| Risparmio energetico da utilizzo di fonti rinnovabili | espresso in KW /anno |
| Risparmio energetico da utilizzo del free-cooling | espresso in KW /anno |

Pur rispondendo a quanto previsto dal requisito **RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore,** indicato nell'allegato dalla determina n.307/2022 emessa dall' Agenzia per la cybersicurezza nazionale con la certificazione ISO 50001, nell'ottica di rispettare lo spirito della specifica **ISO 14064-1 ("Greenhouse gases – Part 1: Specification for the quantification, monitoring and reporting of project emissions and removals")** la NewCo implementerà un report di valori di GHG conforme a quanto previsto nei requisiti dello standard. Allo scopo di massimizzare le modalità di verifica, tale report sarà reso accessibile al Committente.

La NewCo, in presenza di eventuali non conformità, provvederà a sanarle entro i tempi previsti della relativa normativa.

## 17.6 ISO 14001

La strategia introdotta dalla NewCo al fine di massimizzare l'efficacia delle modalità di verifica del rispetto di quanto richiesto dalla ISO 14001 è articolata su quattro pillar:

1. certificazione di tutti i Data Center da cui saranno erogati i servizi relativi al PSN, in ambito Industry Standard;
2. implementazione di uno specifico processo di audit (c.d. Audit Right), al fine di permettere, la verifica da parte del Concedente del rispetto delle relative norme e prescrizioni;
3. possibilità di coinvolgimento del Concedente nelle principali fasi del processo di verifiche interne previsto, in carico alla NewCo, dallo "schema" di certificazione;
4. condivisione con il Concedente dell'avanzamento del programma di certificazione.

In relazione al primo pillar, il processo di mantenimento/rinnovo della certificazione dei Data Center proposti, i cui risultati e certificati saranno condivisi con il Concedente, sarà concluso entro il 2022. Tale certificazione permetterà inoltre di rispondere a quanto richiesto dal **criterio RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore**, indicato nell'allegato dalla determina n.307/2022 emessa dall' Agenzia per la cybersicurezza nazionale.

In relazione al secondo pillar, la NewCo darà la possibilità alla Committente, in parallelo al processo connesso al mantenimento/rinnovo della Certificazione, di effettuare la verifica di quanto previsto dalla relativa normativa mediante una specifica attività di audit. Tale attività, effettuata dal CdC avrà frequenza massima annuale e dovrà avvenire con un preavviso di almeno 30gg.

In relazione al terzo pillar, verrà data la possibilità al Concedente di assistere alle principali fasi, in carico alla NewCo, riguardanti l'iter di certificazione. In particolare, il Committente, previa richiesta formulata con un preavviso di almeno 15 gg, potrà partecipare alle:

- periodiche riunioni di avanzamento relative al programma di certificazione;
- attività di controllo previste dall'iter di certificazione.

In relazione al quarto pillar, la NewCo invierà al Committente:

- il programma (c.d Gantt) di mantenimento/rinnovo della Certificazione con i principali task previsti dal programma stesso;
- un avanzamento, con cadenza trimestrale, delle attività svolte.

## 17.7 SWD (2020) 55 final

La NewCo, al fine di rispettare i requisiti espressi nel documento “COMMISSION STAFF WORKING DOCUMENT - n. 55 final” dal titolo “EU green public procurement criteria for data centres, server rooms and cloud services” - file "SWD (2020)55_0.pdf" emesso dalla Commissione Europea si impegnerà a:

- adottare una specifica policy interna, condivisa con il Concedente, allo scopo di considerare e gestire gli impatti ambientali, economici e sociali delle proprie operatività, attraverso l’implementazione di soluzioni sostenibili e a far rientrare tali impatti tra i fattori decisionali considerati dal proprio personale e dai propri partner;
- adottare una specifica policy interna, condivisa con il Concedente, in cui la NewCo si impegna nella definizione dei presupposti di natura sociale ed etica della negoziazione nei rapporti con i fornitori e all’approfondimento ed aggiornamento dei principi che caratterizzano l’economia circolare, al fine di perfezionare la valutazione dell'impatto socio-ambientale di specifiche categorie di prodotti;
- utilizzare fonti di energia rinnovabile, garantite dal certificato GO fornito da GSE, in conformità con la Direttiva 2009/28/CE;
- soddisfare nei Data Center del PSN i criteri del FINAL TECHNICAL REPORT del Development of the EU Green Public Procurement (GPP) Criteria for Data Centers, Server Rooms and Cloud Services.

In particolare, in ambito procurement, la NewCo si impegna a:

- collaborare con i fornitori per migliorare continuamente le prestazioni di sostenibilità collettiva;
- identificare e rivedere i rischi e gli impatti sulla sostenibilità, dei prodotti e dei servizi acquistati;
- integrare la sostenibilità all'interno dei documenti di gara assicurando che questi siano una parte proporzionata dei criteri di valutazione per gli appalti ad impatto significativo, ove applicabile;
- formare e sviluppare strumenti pratici per aumentare la consapevolezza, la conoscenza e la comprensione delle questioni rilevanti di sostenibilità;
- richiedere la puntuale e costante adozione di un comportamento etico nelle relazioni commerciali nella intera catena di approvvigionamento;
- considerare e valutare i costi dell’intero ciclo di vita (TCO) prima dell'acquisto, ove applicabile;
- ridurre al minimo l'uso di energia e risorse naturali e massimizzare l'uso delle fonti energetiche rinnovabili;

- promuovere soluzioni che consentano significative riduzioni delle emissioni di gas serra nella catena di approvvigionamento, sia nel settore manifatturiero che in quello tecnico, sia nella vita dei prodotti che dei servizi acquistati;
- utilizzare e smaltire i prodotti in modo responsabile dal punto di vista ambientale, compresa la possibilità di ridurre, sostituire, riutilizzare e riciclare, come opzioni sostenibili;
- collaborare con i fornitori /partner per l'abbattimento del rischio di incidenti di sicurezza su tutte le attività svolte con l'auspicabile obiettivo di azzerarli;
- promuovere pratiche di lavoro eque, tra cui la non discriminazione;
- richiedere ai fornitori di garantire i più elevati standard in materia di salute e sicurezza sul posto di lavoro al fine di prevenire e ridurre efficacemente i rischi e i danni ai loro lavoratori.

Al fine di massimizzare l'efficienza nel controllare il rispetto di tali procedure e dei requisiti espressi dalla Commissione Europea, la NewCo propone una strategia basata su due pillar:

- coinvolgimento dei rappresentanti del Concedente nel processo di procurement/iscrizione albo fornitori;
- messa a disposizione al Concedente di report e strumenti atti a verificare il raggiungimento degli obiettivi di efficientamento energetico richiesto da tali norme.

Riguardo al primo pillar, la NewCo intende coinvolgere un rappresentante del Concedente ed eventualmente dell'AgID nelle attività di:

- audit sui fornitori, nel quadro dell'iniziativa Joint Audit Cooperation – JAC (http://jac-initiative.com) collettivo di società di telecomunicazioni che mirano a promuovere condizioni di lavoro sicure ed eque, nonché una gestione responsabile, sociale e ambientale, verificando, valutando e promuovendo gli standard di sostenibilità e il trasferimento delle best practices attraverso la sua catena di fornitura.

Nel caso tali controlli dessero esito negativo, la NewCo adotterà adeguate misure correttive secondo le disposizioni dei contratti al fine di garantire che i requisiti di sostenibilità stabiliti nelle linee guida e nel protocollo JAC siano rispettati, che saranno condivise con il Concedente.

In relazione al secondo pillar, saranno messi a disposizione del Concedente:

- dichiarazione annuale del Trader che fornisce le quote di GO in relazione al consumo di energia prelevata dalla rete elettrica;

- messa a disposizione dell'evidenza di annullamento annuale (anno N) della quota di GO acquistata dopo la scadenza del 31 marzo dell'anno successivo (N-1);
- report annuale della quota parte dell'energia proveniente da fonti rinnovabili;
- report sull'andamento dei contratti di fornitura che rispettano le policy di sostenibilità.

## 17.8 Indipendenza energetica e fonti rinnovabili

La NewCo si propone come società avente lo scopo di conseguire un impatto positivo sulla Società e sulla biosfera, introducendo politiche e norme aziendali che impegnano il management ad azioni di responsabilità ambientale verso principi di sostenibilità ed efficienza energetica.



In tale contesto verrà definita una Politica Energetica aziendale che, attraverso la funzione di Facility Management (Rif. Cap. §19 relativo al Criterio ID 17), si impegnerà a perseguire una continua riduzione dei consumi elettrici e delle emissioni di CO2, nonché a migliorare e garantire l'efficienza energetica dei siti di propria responsabilità. A tal fine verrà implementato un Sistema di Gestione dell'energia conforme ai requisiti della norma ISO 50001:2018 (sia la norma sia l'efficacia delle modalità di verifica sono state precedente descritte), ed applicabile ai siti Data Center costituenti l'infrastruttura gestita dalla NewCo stessa.

La Politica Energetica sarà composta da principi cardine che sono da considerarsi come elementi imprescindibili all'ottenimento di una sempre maggiore efficienza energetica e si identificano nei seguenti punti:

- la conformità ai requisiti legislativi applicabili, attuali e futuri in materia energetica e requisiti volontari sottoscritti;
- la disponibilità di informazioni, risorse umane, tecnologiche e finanziarie;
- la diffusione del documento della Politica Energetica e delle best practice aziendali in tema di utilizzo efficiente dell'energia.

Gli obiettivi che la NewCo intende perseguire sono:

- ottimizzare l'uso e l'acquisto di risorse energetiche attraverso un controllo costante sui consumi;

- ricercare e adottare, ove economicamente conveniente, le migliori tecnologie disponibili sul mercato per migliorare le performances energetiche;
- promuovere e sostenere programmi pluriennali di risparmio energetico;
- progettare i nuovi prodotti e servizi minimizzando i consumi energetici;
- informare e responsabilizzare in maniera continua e costante il personale e i fornitori dei target definiti;
- comunicare e diffondere in maniera sistematica, puntuale e affidabile i dati sulle performances energetiche dell'azienda.

L'efficacia delle verifiche e del raggiungimento degli obiettivi e dei traguardi di efficienza energetica è garantita da interventi da parte delle funzioni di staff che individuano e rivedono periodicamente gli obiettivi quali-quantitativi in un'ottica di miglioramento continuo e di ampliamento dello scope.

Inoltre, la Politica Energetica verrà riesaminata con cadenza minima annuale o in occasione di significative modifiche ai siti, ai sistemi, ai processi e attrezzature, al fine di garantire nel tempo l'adeguatezza alla natura ed alla dimensione.

Come ulteriore validazione della efficacia delle verifiche e del soddisfacimento degli obiettivi che la NewCo intende perseguire in termini di energia rinnovabile, sarà possibile richiedere a società terze un'indicazione sui livelli di fornitura. Tale indicazione, riferita al prelievo di energia elettrica di un intero anno, evidenzierà che la società NewCo si sarà approvvigionata e, conseguentemente, annullerà una quantità di GO pari alla totalità dell'energia elettrica prelevata da rete presso le proprie sedi, come previsto dalla normativa vigente di cui alla Delibera ARERA ARG/elt n. 104/11 e s.m.i. e alle relative istruzioni del GSE.

## 17.9 Direttiva sulla progettazione ecocompatibile (Direttiva 2009/125/CE)

La strategia introdotta dalla NewCo al fine di massimizzare l'efficacia delle modalità di verifica del rispetto di quanto richiesto dalla Direttiva 2009/125/CE prevede l'inserimento di criteri di efficienza energetica all'interno delle policy di acquisto/progettazione.

La Direttiva Europea 2009/125/CE (e di relativi Regolamenti delegati di attuazione) stabilisce come i prodotti devono essere progettati e fabbricati per ridurre il consumo energetico (ci si riferisce in tal caso a Ecodesign o ERP - Energy Related Products). Riconoscendo a questi prodotti un gran consumo di risorse naturali e di energia all'interno della Comunità, nonché un rilevante impatto ambientale, la Direttiva mira a:

- migliorarne l'efficienza energetica;

- ridurne l'impatto ambientale per conseguire un elevato livello di protezione ambientale;
- favorire lo sviluppo sostenibile;
- conseguire un beneficio comune per consumatori e utilizzatori finali.




***Figura 6 Direttiva 2009/125/CE***

Ciascun obiettivo è perseguito attraverso l'armonizzazione delle normative nazionali comportando la necessità di definire requisiti minimi per la progettazione ecocompatibile (eco-design) che i prodotti significativi connessi all'energia devono rispettare per essere immessi sul mercato, garantendone così la libera circolazione.

In queste normative, inclusa la direttiva Europea 2009/125/CE, vengono coinvolti tutti gli apparati di capillare diffusione che consumano energia, dalle lampade agli elettrodomestici ad apparati industriali.

La NewCo individua delle checklist al fine di includere in modo sistematico aspetti di sostenibilità (ambientale e sociale) nelle specifiche tecniche e nelle richieste di acquisto di prodotti e servizi. Maggiori dettagli sono stati riportati nei paragrafi successivi.

La priorità sarà quella di indirizzare tutti quei progetti che coinvolgono:

- sistemi per la circolazione di acqua o aria (es: ventilatori, pompe);
- sistemi di raffrescamento (es: condizionatori, pompe di calore);
- sistemi di riscaldamento: (es: caldaie, pompe di calore);
- unità di trattamento aria;
- sistemi di alimentazione di apparati TLC (es: stazioni energia);
- lampade ed illuminazione in generale.

e che includeranno tra i criteri di progettazione ed acquisto, la valutazione delle performance energetiche durante tutto il loro ciclo di vita.

La NewCo ottempera ad alcune regole per la gestione corretta dei progetti di cui la funzione stessa è responsabile. Per ogni intervento di efficientamento energetico sulle sedi, vengono valutate le prestazioni energetiche degli elementi in oggetto e i risultati della valutazione vengono inseriti nelle specifiche e nelle attività di progettazione ed acquisto. Dunque, si provvede a:

- **definire i requisiti** funzionali al raggiungimento degli obiettivi di performance energetiche definite e le linee guida per la gestione delle attività di progettazione;
- **definire le baseline di consumo** e gli obiettivi e i target richiesti e i relativi KPI;
- **definire le modalità di monitoraggio** e controllo delle performance energetiche;
- **effettuare riesame dei requisiti** di progettazione, acquisto e realizzazione, assieme alle funzioni responsabili della realizzazione dell'attività, proponendo variazioni nel caso i requisiti di performance energetica non siano sufficienti a garantire gli obiettivi prestabiliti al fine di garantire il rispetto della Politica Energetica, degli obiettivi e dei target definiti;
- **verificare a collaudo avvenuto le performance** reali rispetto a quelle attese tramite i KPI definiti;
- **richiedere alla funzione responsabile** della realizzazione/conduzione le modifiche necessarie a garantire il rispetto dei target definiti nel caso in cui durante la fase di esercizio, dovessero emergere delle incongruenze rispetto ai risultati delle valutazioni di performance energetiche e agli obiettivi energetici definiti.

L'acquisto, così come la progettazione, rappresenta un'altra opportunità per migliorare la prestazione energetica attraverso l'utilizzo di prodotti e servizi più efficienti. Esso è anche un'opportunità per lavorare con la catena di fornitura ed influenzare il suo comportamento energetico in maniera virtuosa:

- la policy di acquisto di prodotti e servizi contiene indicazioni per acquisti sostenibili anche dal punto di vista dell'efficienza energetica;
- la qualifica dei fornitori della NewCo prevede una valutazione dal punto di vista della sostenibilità.

Di seguito è delineato l'approccio da seguire nel processo di acquisto definito, in coerenza con i principi del Codice Etico e di Condotta della NewCo, sulla base dei risultati di una serie di iniziative avviate dal costituito RTI, attraverso un processo di coinvolgimento delle parti interessate, che hanno portato – tra l'altro – alla definizione dei presupposti di natura sociale ed etica della negoziazione nei rapporti tra la NewCo ed i fornitori e all'approfondimento ed aggiornamento dei principi che caratterizzano l'economia

circolare, al fine di perfezionare la valutazione dell'impatto socio-ambientale di specifiche categorie di prodotti.

Il livello di conformità ai principi ivi riportati è valutato e misurato nei processi di valutazione/controllo dei fornitori e nella selezione di servizi/prodotti, con metodi operativi specifici per ciascuna categoria di acquisizione/fornitore.

La NewCo effettuerà controlli, direttamente o attraverso organismi esterni:

- sulla corrispondenza dei prodotti/servizi acquisiti con la presente politica e con le procedure applicative, sui prodotti durante la fase di validazione del prototipo e sulla base di campioni per produzioni di serie;
- sui fornitori, anche in cooperazione e attraverso accordi con partner o altri operatori di telecomunicazioni al fine di verificare, valutare e promuovere gli standard di sostenibilità e il trasferimento delle *best practices* attraverso la sua catena di fornitura.

Se i controlli daranno esiti negativi, verranno adottate adeguate misure correttive secondo le disposizioni dei contratti al fine di garantire che i requisiti di sostenibilità stabiliti nelle linee guida vengano soddisfatti.

### Promozione delle best practice in ambito di sostenibilità

La NewCo si impegna a incoraggiare la continua ricerca da parte dei fornitori di soluzioni tecnologiche innovative nel campo della sostenibilità ambientale, oltre alla sostenibilità sociale ed economica, promuovendo le best practice e tenendone debitamente conto nella metodologia di Vendor Rating. Nei casi in cui tali requisiti non siano adeguatamente soddisfatti dai fornitori e/o partner, la NewCo:

- segnalerà loro l'area di miglioramento rilevata richiedendo l'adeguamento entro il termine condiviso;
- ove opportuno, e ferma l'autonoma responsabilità del fornitore/partner, potrà consentire il loro accesso a specifiche attività di formazione, nell'ottica di un rapporto di reciproca collaborazione.

### I Principi alla base dell'impegno di Procurement per la Sostenibilità

La NewCo provvede ad assicurare le seguenti attività:

- incoraggiare e coinvolgere i fornitori per sviluppare un approccio proattivo ai problemi di sostenibilità e fornire soluzioni sostenibili;
- collaborare con i fornitori per migliorare continuamente le prestazioni di sostenibilità collettiva;

- identificare e rivedere i rischi e gli impatti sulla sostenibilità, dei prodotti e dei servizi acquistati;
- formare e sviluppare strumenti pratici per aumentare la consapevolezza, la conoscenza e la comprensione delle questioni rilevanti di sostenibilità;
- richiedere la puntuale e costante adozione di un comportamento etico nelle relazioni commerciali nella intera catena di approvvigionamento;
- considerare e valutare i costi dell'intero ciclo di vita (TCO) prima dell'acquisto, ove applicabile;
- ridurre al minimo l'uso di energia e risorse naturali e massimizzare l'uso delle fonti energetiche rinnovabili;
- promuovere soluzioni che consentano significative riduzioni delle emissioni di gas serra nella catena di approvvigionamento, sia nel settore manifatturiero che in quello tecnico, sia nella vita dei prodotti che dei servizi acquistati;
- utilizzare e smaltire i prodotti in modo responsabile dal punto di vista ambientale, compresa la possibilità di ridurre, sostituire, riutilizzare e riciclare, come opzioni sostenibili;
- collaborare con i fornitori /partner per l'abbattimento del rischio di incidenti di sicurezza su tutte le attività svolte con l'auspicabile obiettivo di azzerarli;
- promuovere pratiche di lavoro eque, tra cui la non discriminazione;
- richiedere ai fornitori di garantire i più elevati standard in materia di salute e sicurezza sul posto di lavoro al fine di prevenire e ridurre efficacemente i rischi e i danni ai loro lavoratori.

### 17.10 Le apparecchiature elettriche acquistate non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva (Direttiva RoHS)

La NewCo acquisterà apparecchiature elettriche che assolutamente non conterranno le sostanze soggette a restrizione elencate nell'allegato II della direttiva 2011/65/UE in alcun valore di concentrazione in peso in materiali omogenei superiore ai valori massimi elencati in tale direttiva.

Verrà consolidata la check-list di sostenibilità, sotto riportata, che individua i principali parametri ambientali e sociali che rappresentano per la NewCo il riferimento base, rispetto al quale redigere una specifica tecnica e la conseguente richiesta di acquisto. Nel caso di specifiche tecniche funzionali, la check-list consente di definire i requisiti minimi o target di carattere ambientale e sociale che devono essere soddisfatti dal prodotto/servizio richiesto e che ottemperano a quanto riportato dalla Direttiva 2011/65/UE.

La check-list composta da 30 parametri si articola in:

- **fasi del ciclo di vita del prodotto/servizio** che si distinguono in: progettazione/produzione, utilizzo, fine vita;
- **aspetti** che meglio caratterizzano ciascuna fase del ciclo di vita;
- **impatto** in termini di sostenibilità, che può essere ambientale o sociale.

Gli aspetti e i parametri di sostenibilità variano in maniera specifica in base alle caratteristiche dei prodotti/servizi considerati. Per tale motivo, la definizione di ciascun parametro viene adattata al prodotto/servizio all'interno delle specifiche tecniche. A ciascun parametro è possibile associare alternativamente **due valori**:

- **A: requisiti minimi** associabili in prevalenza a provvedimenti legislativi e/o alla normativa obbligatoria ambientale/di sicurezza/sociale di riferimento;
- **B: requisiti target** più sfidanti in termini di sostenibilità, aggiuntivi e di rinforzo ai requisiti minimi (ad es. dal punto di vista di consumo di energia, di emissioni, eco-design).

Per ciascun prodotto/servizio è possibile definire sia il valore minimo che target. All'interno della checklist verrà indicato un solo valore (minimo o target) e nel campo note della checklist il riferimento di pagina del documento tecnico in cui vi è il dettaglio sul valore minimo o target.

Per ciascun parametro è possibile esprimere la non applicabilità al prodotto/servizio richiesto.

| Fase | Aspetti | Impatto | N. | Parametri di sostenibilità | Applicabilità |
|---|---|---|---|---|---|
| | **MATERIALI / ASSEMBLAGGIO** | **ambientale** | 1 | Marchi ambientali | Hardware |
| | | | 2 | Marcatura del prodotto e/o di sue componenti | Hardware |
| | | | 3 | Sostanze ritenute pericolose nel prodotto/sue componenti | Hardware |
| | | | 4 | Inchiostri e vernici ritenute pericolose nel prodotto/sue componenti | Hardware |
| | | | 5 | Modularità del prodotto/sue componenti | Hardware |

| | | | | | |
|---|---|---|---|---|---|
| **PROGETTAZIONE PRODUZIONE** | | | 6 | Minimizzazione del numero di componenti e delle miscele di materiali differenti | Hardware |
| | | | 7 | Materiali riciclati/rigenerati nel prodotto/sue componenti | Hardware |
| | | | 8 | Materiali riciclabili nel prodotto/sue componenti | Hardware |
| | | | 9 | Istruzioni del prodotto | Hardware |
| | **IMBALLAGGI** | **ambientale** | 10 | Marcatura dell'imballaggio | Hardware |
| | | | 11 | Inchiostri e vernici ritenute pericolose nell'imballaggio | Hardware |
| | | | 12 | Materiali riciclati nell'imballaggio primario | Hardware |
| | | | 13 | Materiali riciclati nell'imballaggio secondario/terziario | Hardware |
| | | | 14 | Materiali riciclabili negli imballaggi | Hardware |
| | **MANODOPERA** | **sociale** | 15 | Impiego di materie prime/semilavorati/prodotti di origine locale/nazionale | Hardware |
| | | | 16 | Impiego di manodopera locale | Hardware/Software/Servizi |

| | | | | | |
|---|---|---|---|---|---|
| | | | 17 | Impiego di lavoratori non occasionali o a breve termine | Hardware/Software/Servizi |

| Fase | Aspetti | Impatto | N. | Parametri di sostenibilità | Applicabilità |
|---|---|---|---|---|---|
| UTILIZZO | EMISSIONI | ambientale | 18 | Emissioni in atmosfera e rilasci di sostanze nell'ambiente | Hardware |
| | | | 19 | Emissioni elettromagnetiche | Hardware |
| | | | 20 | Inquinamento acustico | Hardware |
| | CONSUMO ENERGETICO E DI RISORSE | ambientale | 21 | Prestazione energetica | Hardware/Software |
| | | | 22 | Etichettatura sul consumo energetico | Hardware |
| | | | 23 | Contratto a performance energetica garantita | Hardware |
| | | | 24 | Minimizzazione consumo di acqua | Hardware |
| | | | 25 | Affidabilità | Hardware/ Software/Servizi |

| Fase | Aspetti | Impatto | N. | Parametri di sostenibilità | Applicabilità |
|---|---|---|---|---|---|
| | OPZIONI DI FINE VITA | ambientale | 26 | Riparabilità del prodotto/sue componenti | Hardware |

| | | | | | |
|---|---|---|---|---|---|
| **FINE VITA** | | | 27 | Riutilizzo/recupero del prodotto o di sue parti/componenti | Hardware |
| | | | 28 | Re-selling del prodotto o di sue parti/componenti ad un fornitore terzo | Hardware |
| | | | 29 | Riutilizzo/recupero degli imballaggi | Hardware |
| | | | 30 | Smaltimento | Hardware |

### Modalità di utilizzo della check-list

I parametri di sostenibilità indicati nella check-list sono parte integrante dei requisiti previsti nelle specifiche tecniche. In particolare, all'interno di ciascuna specifica tecnica, verrà inserita una sezione dedicata alla sostenibilità con l'inserimento dei parametri associati al prodotto/servizio. Per ciascun parametro dovrà esserci una breve descrizione che ne contestualizza le caratteristiche rispetto al prodotto e verrà poi indicata la non applicabilità o il valore minimo/ target associato. Sulla base del documento di specifiche tecniche così compilato, verrà redatta la check-list che conterrà nel campo note i riferimenti ai paragrafi della specifica tecnica in cui sono stati trattati i diversi parametri di sostenibilità.

La presenza di sostanze pericolose in un prodotto e/o nei suoi componenti permetterà di identificare i materiali, in modo da poterli smaltire correttamente. Non verranno in alcun modo considerati congrui apparati con sostanze pericolose per la salute e l'ambiente secondo la Direttiva RoHS. I prodotti utilizzati dalla NewCo saranno obbligatoriamente conformi alla Direttiva RoHS 2 (Direttiva 2011/65/UE) e RoHS 3 (Direttiva Delegata 2015/863). Affinché venga monitorato il processo di verifica ed ottemperanza a tali direttive:

- nella Dichiarazione di Conformità del prodotto dovrà risultare la conformità alle predette Direttive;
- nel fascicolo tecnico di prodotto dovrà poi essere presente il report redatto in conformità alla norma EN 63000:2018 con l'indicazione della eventuale presenza, tipologia ed il quantitativo di sostanze definite pericolose *(rif. Allegato H del D. Lgs 152 del 03/04/06 e successivi*

*aggiornamenti).* In particolare, dovrà essere indicata con precisione l'eventuale presenza di piombo, mercurio, cadmio, cromo esavalente, polibromuratibifenili PBB, eteri di difenile polibromurato PBDE *e delle altre sostanze pericolose introdotte dalla RoHS3.* Dovrà essere inoltre indicata sulla documentazione di prodotto la presenza delle sostanze pericolose (*D.Lgs. del 14/03/2014 n° 49 "Attuazione della direttiva 2012/19/UE sui rifiuti di apparecchiature elettriche ed elettroniche*).

## Scoring

Alla checklist è associato un sistema di scoring che consente la rilevazione di due KPI:

- grado di applicazione della checklist (% parametri applicabili su totale parametri);
- rating di sostenibilità (% di valori minimi e/o target applicati ai parametri della checklist).

L'algoritmo di calcolo dei due KPI prevede:

- un peso attribuito in modo uniforme alle fasi del ciclo di vita del prodotto (eventualmente differenziabili);
- un punteggio di 0 dato al valore minimo e di 1 dato al valore target.

Di seguito si riporta un esempio di scoring:

| | | | | |
|---|---|---|---|---|
| KPI 1 | APPLICABILITA' DEI PARAMETRI ECOSOSTENIBILI | 58% | | |
| KPI 2 | RATING DI SOSTENIBILITA' | 6% | D | Migliorabile |

| Fase ciclo di vita | Peso | Parametri disponibili | Parametri valutati | Parametri non valutati | % Applicabilità | Punteggio ottenuto | |
|---|---|---|---|---|---|---|---|
| | | | | | | Punti * | % |
| PROGETTAZIONE/PRODUZIONE | 33% | 15 | 2 | 13 | 13% | 1 | 17% |
| UTILIZZO | 33% | 7 | 6 | 1 | 86% | 0 | 0% |
| FINE VITA | 33% | 8 | 6 | 2 | 75% | 0 | 0% |
| | | 30 | 14 | 16 | 58% | 1 | 6% |

* valore A (requisiti minimi): 0 punti; valore B (requisiti tg): 1 punto

| GRADING PUNTEGGIO | | |
|---|---|---|
| CLASSE | DESCRIZIONE | RANGE |
| A | Eccellente | ≥ 90% |
| B | Buono | < 90% e ≥ 60% |
| C | Adeguato | < 60% e ≥ 40% |
| D | Migliorabile | < 40% e ≥ 0% |
| E | Base | = 0% |

***Figura 7 Esempio di scoring***

## 17.11 Procedure di approvvigionamento e Gestione del ciclo di vita delle apparecchiature

In fase di progettazione dell'infrastruttura IT, la NewCo considera anche la possibilità di riutilizzare hardware già disponibile, in base a quanto risulta nel sistema di inventory degli asset IT, dove per Asset IT si intendono Server fisici o virtuali, Sistemi di Storage, Apparati di Networking e Apparati ausiliari.

Il processo di gestione degli asset IT adottato dalla NewCo persegue i seguenti obiettivi:

- standardizzare il censimento degli asset presenti nei Data Center tramite un sistema centralizzato (Inventory Management IT);
- regolamentare e agevolare le analisi di razionalizzazione del livello di utilizzo degli spazi e dei consumi collegati;
- ottimizzare la gestione della connettività, anche ai fini della riduzione dei costi;
- garantire l'affidabilità degli stessi asset, introducendo tutti gli accorgimenti utili allo scopo.

La NewCo si prefigge l'obiettivo di presidiare, in modo continuativo, la gestione degli asset, di effettuare tutte le attività abilitanti al corretto funzionamento del loro ciclo di vita e di garantire la qualità dei dati di configurazione, fornendo gli elementi ed il supporto per la corretta gestione agli attori coinvolti.

In considerazione del carattere altamente dinamico insito nella definizione delle configurazioni e dei volumi gestiti (migliaia di asset), le baseline, in uno stato di validità continuo e garantito, sono costituite dalle righe di registrazione sulla base dati del tool utilizzato a supporto, i cui report possono essere consultati dagli utenti abilitati per la ricerca di asset IT disponibili per il riuso.

In ultima analisi, se l'asset IT richiesto per un determinato progetto non risulta disponibile, oppure lo è ma necessita di componenti aggiuntivi non disponibili, si provvederà al relativo approvvigionamento mediante acquisto.

La NewCo si rende disponibile per l'espletamento di **audit annuali** condotti dal Concedente per il processo qui esposto (previo preavviso di almeno 30 giorni) e la fornitura di reportistica periodica (con frequenza e contenuti da concordare).

Report che NewCo si impegna a fornire:

- report delle consistenze degli asset IT utilizzati dal Concedente, con l'indicazione dei relativi stati asset.

Con riferimento al ciclo di vita delle apparecchiature, la NewCo adotta un processo che prevede un iter di verifica di riutilizzabilità dell'hardware dismesso.

Nel caso di verifica con esito positivo, l'hardware viene destinato a nuovi progetti. L'hardware non riutilizzabile viene alienato e venduto oppure avviato alla rottamazione, in conformità alle direttive di smaltimento dei rifiuti IT di cui all'allegato VII della direttiva 2012/19/UE.

L'attività prevede una verifica sulle caratteristiche dell'asset dismesso allo scopo di destinarlo a:

- riuso;
- scorta (sistema intero o parti componenti);
- rivendita;
- rottamazione.

Qualora l'asset debba essere rottamato occorre verificare, tramite gli specifici attributi dello stesso, il suo completo ammortamento e provvedere alla cancellazione sicura dei dati.

Più in dettaglio, con frequenza semestrale, la NewCo esegue la cosiddetta "certificazione d'uso dell'hardware" che consiste nelle seguenti attività:

- acquisizione dei dati relativi ad apparecchiatura di proprietà (dati di asset inventory, riferimenti applicativi, attività di backup e manutenzione hardware eseguite sulle apparecchiature);
- creazione reportistica ad hoc a supporto della successiva fase di verifica da parte delle funzioni competenti. Ad esempio, l'individuazione degli asset "orfani", i quali presentano l'anomalia di non avere applicazioni associate sul sistema Inventory Management IT, e dei presunti "zombie", i quali presentano l'anomalia di essere associati ad applicazioni per le quali non eroga servizio fattivo;
- verifica di effettivo utilizzo dei server da parte delle funzioni competenti;
- trattamento dei server orfani e degli zombie; è prevista l'applicazione di una procedura di dismissione controllata con quarantena per migliorare l'affidabilità del processo;
- registrazione dell'esito della certificazione HW nello strumento Inventory Management.

L'hardware non certificato (ovvero, non utilizzato da alcuna applicazione) viene successivamente sottoposto a verifica per stabilire se possiede caratteristiche tali per cui può essere riutilizzato ("Reborn") o se, invece, deve essere rottamato.

Il macro-flusso seguente (Figura 8) rappresenta, sinteticamente, le fasi di certificazione HW, dismissione e disassociazione dalle applicazioni e analisi per il riuso.

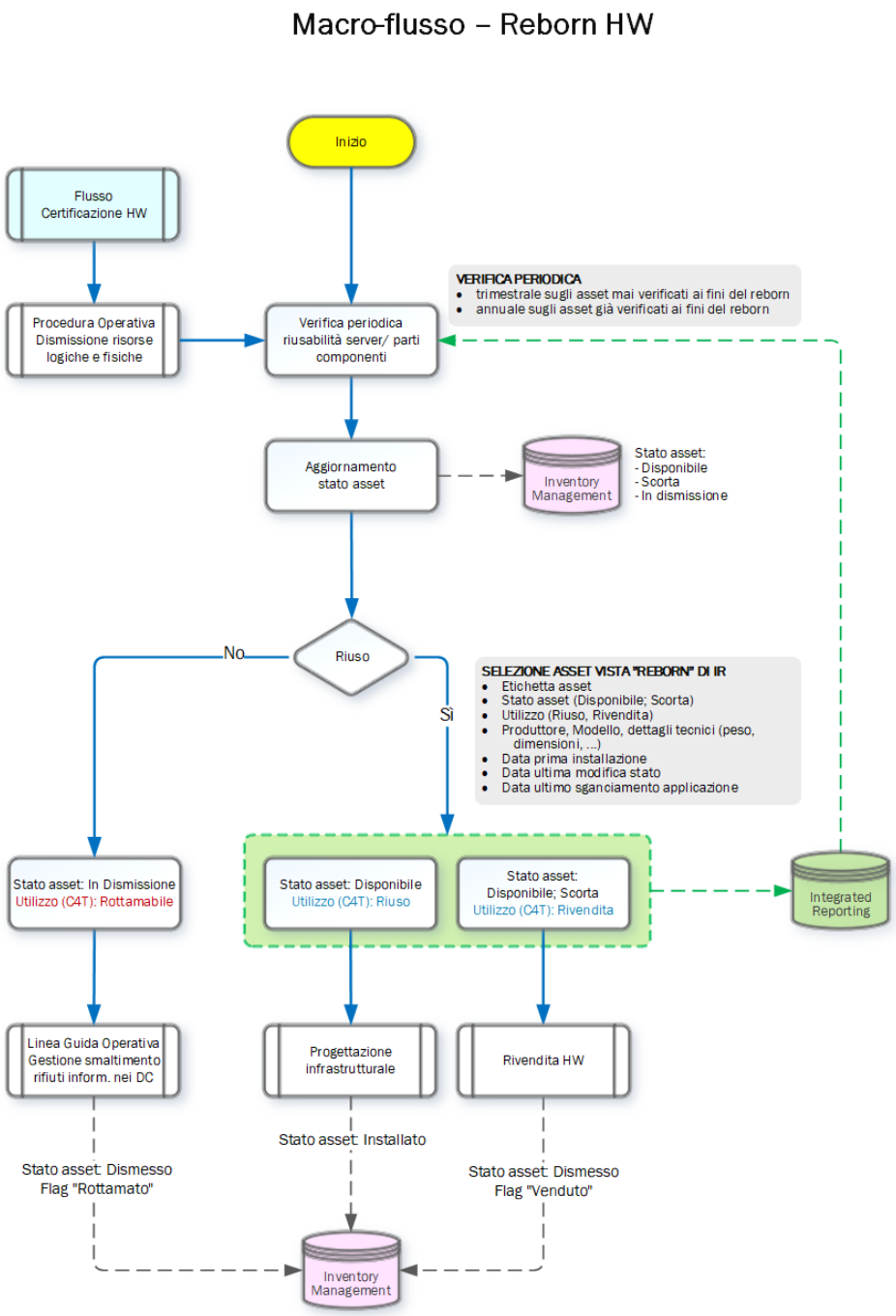



**Figura 8 Macro-flusso - Reborn HW**

In riferimento a quanto esposto, la NewCo si rende disponibile per:

- applicare tale processo all'hardware a servizio del Concedente con modalità da concordare;

- espletare audit annuali condotti dal Concedente (previo preavviso di almeno 30 giorni) e fornire reportistica periodica (con frequenza e contenuti da concordare).

Report che NewCo si impegna a fornire:

- report degli asset IT riutilizzabili.

# 18 ID 16 – Valutativo - Miglioramenti, a favore del Concedente, della matrice di ripartizione del rischio. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili

## 18.1 Executive Summary

In relazione ai miglioramenti sugli aspetti di ripartizione dei rischi di cui al criterio valutativo 16 del disciplinare di gara, il costituito RTI propone i seguenti cambiamenti a beneficio del concedente:

- rischio "Domanda": abbassamento del valore del TIR di progetto target ai fini del riequilibrio da un valore di 5,1% ad un valore di 4,6% con conseguente riduzione dell'impegno dell'amministrazione in caso di riequilibrio del PEF in misura pari alla differenza tra il TIR di progetto attuale e il nuovo valore di riequilibrio proposto (i.e. differenza pari a 0,5%);
- rischio "Forza Maggiore": introduzione di una soglia di tolleranza (fino al limite dello 0,20%) rispetto alle alterazioni dell'equilibrio calcolate attraverso la variazione del TIR del Progetto con conseguente condivisione del rischio da parte del concessionario, diversamente da quanto previsto dall'attuale matrice dei rischi (i.e. rischio "Forza Maggiore" interamente in capo al concedente);
- rischio "Mutamenti imposti ex lege": incremento della soglia di tolleranza da un valore di 0,15% ad un valore di 0,20% rispetto alle alterazioni dell'equilibrio calcolate attraverso la variazione del TIR del Progetto con conseguente assunzione di un rischio maggiore in capo al concessionario.

Di seguito si riporta una versione della matrice dei rischi posta a base di gara, aggiornata alla luce dei miglioramenti previsti.

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di domanda** | Rischio di domanda relativo al numero di Amministrazioni utenti che decideranno di migrare nonché alla quantità e tipologia di servizi che le stesse richiederanno | Alta | Diminuzione dei ricavi e dei costi parametrati ai volumi. Contestuale riduzione del MOL, dell'utile netto e del TIR. | Obbligo per le PA di rimborsare il PSN dei i costi sostenuti ed eventualmente corrispondere una fee a parziale copertura dei mancati ricavi In caso di early termination.<br>Riequilibrio del PEF in caso di rendimento inferiori alla soglia individuata. | Abbassamento, nel caso di rischio di domanda, del valore del TIR di progetto target ai fini del riequilibrio a 4,6% ✓ | ✓ | Art. 5;<br>Art. 9, comma 1, lett. a);<br>Art. 10,<br>Art. 11. |
| **Forza Maggiore** | Forza maggiore che comporti modifica del Piano Economico-Finanziario. | Minima | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | Introduzione di una soglia di tolleranza rispetto alle alterazioni dell'equilibrio fino allo 0,20% del TIR ✓ | ✓ | Art. 11;<br>Art. 19;<br>Art. 37. |
| **Mutamenti imposti ex lege** | Mutamenti imposti ex lege (ivi compresi mutamenti relativi ad innovazioni tecnologiche, strumenti e/o tecniche diverse) che comportino modifica del PEF | Media | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | Incremento della soglia di tolleranza rispetto alle alterazioni dell'equilibrio fino allo 0,20% del TIR ✓ | ✓ | Art. 5;<br>Art. 11;<br>Art. 37. |

Miglioramento introdotto  Proposta di condivisione del rischio

**Figura 9 Matrice dei rischi**

In aggiunta a quanto sopra, di seguito si fornisce un approfondimento rispetto ai miglioramenti proposti.

## 18.2 Rischio "Domanda"

La matrice dei rischi allegata allo "schema di convenzione" posto a base di gara prevede l'allocazione del rischio di "*domanda*" come parzialmente condiviso.

Tale rischio è rappresentato dalla non prevedibilità (a) del numero di Amministrazioni utenti che dovessero decidere di migrare; nonché (b) della quantità e tipologia dei servizi che le stesse potranno richiedere.

Gli effetti di tale rischio si manifestano attraverso una riduzione dei ricavi (e, fermi i costi fissi, dei connessi costi parametrati ai volumi), con contestuale riduzione del MOL, dell'utile netto e del TIR.

Al riguardo, in coerenza con il principio di parziale condivisione del rischio recepito in sede di valutazione di fattibilità della proposta, la bozza corrente dello "schema di convenzione" prevede che il verificarsi di fatti non riconducibili al concessionario che incidano sull'equilibro economico finanziario non comportino automaticamente la revisione del piano economico finanziario volta alla rideterminazione delle condizioni di equilibrio.

Tale conseguenza è collegata esclusivamente ad una significativa alterazione del TIR di progetto (i.e. inferiore al 2,4%); in particolare, la bozza corrente dello "schema di convenzione" (cfr. articolo 11 (*Revisione del PEF*), quinto comma) dispone che:

5. *Le Parti, fatto salvo quanto previsto ai commi 8 e 10, convengono di procedere alla revisione del PEF contrattuale e della Convenzione, oltre che al verificarsi di una Variazione dell'Equilibrio dovuta a una delle fattispecie di cui al comma 4, anche laddove, al trentesimo (30°) mese dalla stipula della presente Convenzione, per effetto di un evento non imputabile al Concessionario la Variazione dell'Equilibrio determini un TIR di progetto, al netto delle imposte, inferiore al 2,4% (due virgola quattro per cento).*

In presenza di tale circostanza (i.e. TIR del progetto inferiore al 2,4%), il meccanismo di revisione del PEF attualmente previsto opera in via ordinaria, con obbligo di ripristinare i livelli che concorrono alla formazione dell'Equilibrio Economico Finanziario e pertanto, quanto al TIR del progetto, di avere un valore pari al 5,1% (cfr. art. 11 (*Revisione del PEF*), commi primo, secondo e terzo).

Il costituito RTI, a maggior tutela e vantaggio del Concedente, propone di migliorare l'impostazione attuale prevedendo che, in deroga alla procedura di revisione ordinaria del PEF, per l'ipotesi in parola (e limitatamente ad essa) il valore del TIR di progetto *target* ai fini del riequilibrio sia collocato ad un livello inferiore, pari al 4,6%. Di conseguenza, in presenza delle relative circostanze, l'impegno dell'amministrazione sarebbe ridotto in misura pari alla differenza tra il TIR di progetto di equilibrio e quello, più modesto, che il Concessionario si rende disponibile considerare come livello *target* contingente (i.e. differenza pari a 0,5%).

La procedura di revisione del PEF contrattuale non determinerebbe una modifica in riduzione del livello del TIR del progetto che concorre all'Equilibrio Economico Finanziario (che resterebbe, pertanto, contrattualmente convenuto al 5,1%). Laddove ne ricorrano i relativi presupposti, pertanto, i futuri flussi di cassa generati dal progetto restano asserviti alla copertura dei fabbisogni del Concessionario e potranno concorrere a riportare il parametro di redditività ai livelli di equilibrio (i.e. 5,1%). Del pari, eventuali future e diverse Variazioni dell'Equilibrio dipendenti dal verificarsi delle fattispecie indicate all'articolo 11 (*Revisione del PEF*), comma quarto) potranno comportare l'attivazione della procedura di revisione del PEF contrattuale volta a ripristinare il livello degli Indicatori di Equilibrio (i.e. TIR del progetto 5,1%; DSCR minimo, almeno pari a 1,4X).

La misura descritta è chiaramente a beneficio del Concedente. Essa è evidente ed oggettiva, incrementando la quota di "rischio" a carico del Concessionario rispetto alla disciplina corrente. È inoltre chiara e misurabile, essendo calcolata mediante ricorso allo stesso strumento contrattuale utilizzato dalle parti per valutare l'Equilibrio Economico Finanziario.

## 18.3 Rischio "Forza Maggiore"

La matrice dei rischi allegata allo "schema di convenzione" posto a base di gara prevede l'allocazione del rischio di "*Forza Maggiore*" esclusivamente in capo al Concedente.

In particolare, la bozza corrente dello "schema di convenzione" prevede che il verificarsi di un evento "Forza Maggiore", cui sia connessa una "Variazione dell'Equilibrio", comporti l'attivazione della procedura di Revisione del PEF.

Al riguardo, si propone di migliorare l'impostazione corrente, a maggior tutela e vantaggio del Concedente, riconfigurando l'allocazione del rischio come "condiviso".

Sotto il profilo tecnico, tale risultato viene perseguito in maniera evidente, oggettiva e misurabile attraverso l'introduzione di una soglia di tolleranza (fino al limite dello 0,20%) rispetto alle alterazioni dell'equilibrio calcolate attraverso la variazione del TIR del Progetto.

Sul piano redazionale, si ipotizza una riformulazione dell'articolo 11 (*Revisione del PEF*), quarto comma, dello "schema di convenzione", volto a riflettere l'inserimento della soglia di tolleranza.

La misura descritta è chiaramente a beneficio del Concedente, ponendo il "primo rischio" dipendente dal verificarsi di un evento di "Forza Maggiore", a carico del Concessionario.

## 18.4 Rischio "Mutamenti imposti ex lege"

La matrice dei rischi allegata allo "schema di convenzione" posto a base di gara prevede l'allocazione del rischio di "*mutamenti imposti ex lege*" come parzialmente condiviso.

Al riguardo, la bozza corrente dello "schema di convenzione" prevede che

*"l'entrata in vigore di norme legislative e regolamentari che incidano sui termini e sulle condizioni di progettazione, predisposizione ed ammodernamento quinquennale dell'infrastruttura nonché di prestazione del Servizio, in particolare, sui costi o i tempi dello stesso",*

comportino l'attivazione della procedura di Revisione del PEF, nel caso in cui i mutamenti normativi abbiano comportato una variazione negativa del TIR del progetto superiore allo 0,15%.

Al riguardo, si propone di migliorare ulteriormente l'impostazione corrente, a maggior tutela e vantaggio del Concedente, incrementando la soglia di tolleranza (che verrebbe portata al più elevato valore dello 0,20%) rispetto alle alterazioni dell'equilibrio calcolate attraverso la variazione del TIR del Progetto.

Sotto il profilo tecnico, tale risultato verrebbe pertanto perseguito in maniera evidente, oggettiva e misurabile attraverso l'incremento della soglia di tolleranza.

Sul piano redazionale, si ipotizza una riformulazione dell'articolo 11 (*Revisione del PEF*), quarto comma, lettera (c) dello "schema di convenzione", volto a riflettere l'incremento della soglia di tolleranza.

La misura descritta è chiaramente a beneficio del Concedente, incrementando la quota di "primo rischio" dipendente dal verificarsi di un evento di "*change in law*", a carico del Concessionario.

# 19 ID 17 – Valutativo - Miglioramenti del modello di governance utili a consentire un maggior coinvolgimento del Concedente anche nell'ottica di garantire ulteriormente la vigilanza e il monitoraggio pubblico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili

## 19.1 Executive Summary

Il modello organizzativo proposto, in relazione alla premialità sui miglioramenti degli aspetti di governance, rappresenta un miglioramento ed un completamento di quanto descritto nei documenti di gara, ed in particolare nel paragrafo 2.6 dell'Allegato 3 sub 2 Specificazione caratteristiche servizio e gestione con allegato 2.0.

Nella definizione del modello organizzativo per il governo e per l'erogazione dei servizi, il Costituito RTI intende adottare un approccio unitario e integrato, in grado di far corrispondere le potenzialità dei servizi proposti con le esigenze delle Amministrazioni e di accompagnare queste ultime verso l'adozione di soluzioni mirate al paradigma della migrazione in Cloud, in pieno rispetto del criterio ID 17 riportato nel Disciplinare di gara PSN (1) signed, tabella n.5, pag. 42.

Viene definito un modello operativo in cui convivono capacità operative, competenze, servizi innovativi e diffusione sul territorio, in grado di portare innovazione ed efficientamento nelle singole PPAA, al fine di garantire la vigilanza e il monitoraggio pubblico.

## 19.2 Governance

Il modello organizzativo proposto, raffigurato come modello logico in Figura 10, ha l'obiettivo sia di assicurare al DTD ed alle Amministrazioni Aderenti un governo efficace dei contratti ed un'erogazione puntuale dei servizi, sia di favorire la diffusione dei servizi oggetto della Convenzione presso le Amministrazioni Aderenti. Ciò si sostanzia in un modello di Governance integrato a due livelli, uno per

la gestione della Convenzione ed uno per i singoli Contratti di Adesione (CA), in cui alcuni processi trasversali considerati critici, quali la gestione della qualità, della sicurezza e degli SLA, sono centralizzati.

La **Figura *10*** evidenzia come venga posta grande attenzione non soltanto alle tematiche operative di governo ed erogazione dei servizi ma anche ad aspetti di contesto specifico quali la Diffusione ed Evoluzione della Convenzione e la Risposta ai CA.




**Figura 10 Modello di Governance**

Tale framework di riferimento permette di definire un modello organizzativo in grado di adattarsi in maniera flessibile alle diverse tipologie di Amministrazioni Aderenti e al contesto territoriale di riferimento, permettendo una gestione ottimale della contemporaneità delle richieste e dei picchi di lavoro ed assicurando una gestione dinamica delle risorse, umane e tecnologiche, utile a rendere sostenibile la soluzione proposta. Nella sua formulazione si è tenuto, quindi, conto delle diverse tipologie di servizio che possono essere previste nell'ambito dei vari CA, degli ambiti tecnologici, funzionali e tematici di interesse, delle diverse modalità e luoghi di erogazione dei servizi, delle fasce di erogazione e SLA richiesti e, più generale, delle specifiche esigenze che ciascuna Amministrazione Aderente potrà esprimere, di volta in volta, attraverso i singoli CA.

Il modello organizzativo proposto, rappresentato nella figura sottostante, si pone l'obiettivo di indirizzare in modo unico ed integrato le tematiche di governo ed erogazione dei servizi congiuntamente alla fase

di Gestione dell'Offerta, propedeutica alla sottoscrizione dei CA, dando evidenza delle relazioni con il DTD e con la singola PA.

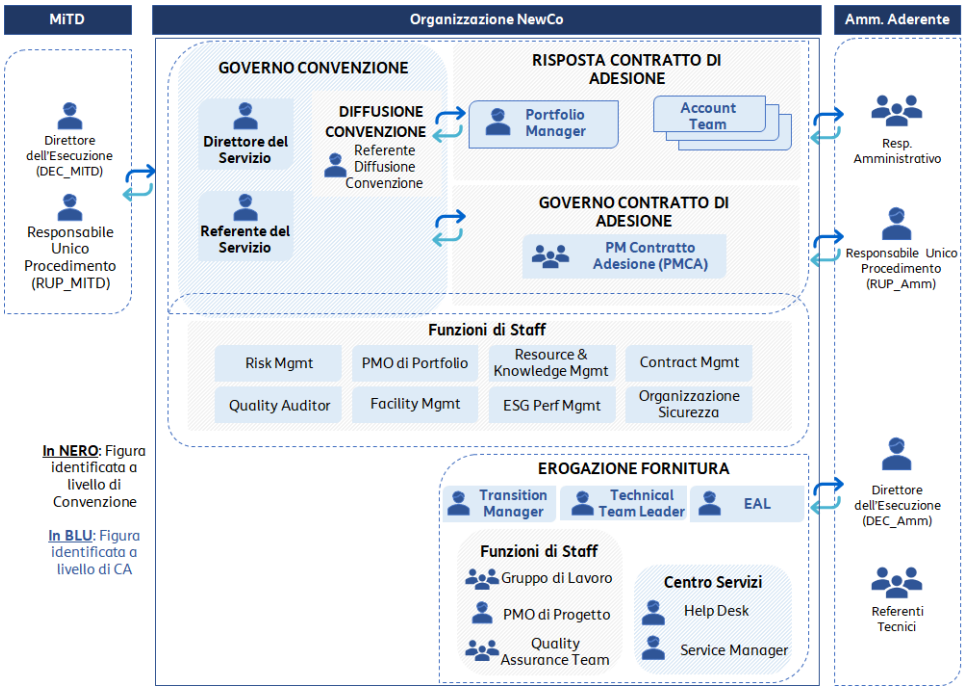



**Figura 11 Modello Organizzativo**

Nel seguito vengono descritte in dettaglio le sezioni che compongono il modello organizzativo sopra rappresentato.

## 19.3 Governo della Convenzione e figure a supporto

Il modello di governance proposto prevede una **figura unica di riferimento per l'intera Convenzione**, con esperienza pluriennale nella gestione di Convenzioni ed Accordi Quadro di grande rilevanza, il **Referente del Servizio.** Esso ricopre i ruoli previsti dalle practice ITIL V4 di Business Relationship Manager, Demand Manager, Financial Manager, Service Portfolio Manager, a livello di Convenzione, svolgendo le seguenti attività:

- responsabile per la NewCo del coordinamento e del controllo dell'intera Convenzione per tutte le attività contrattuali previste, al fine di indirizzarne e verificarne l'andamento;
- punto di coordinamento ed escalation nel governo dei singoli appalti e contratti;
- controlla e verifica i singoli CA per garantire il rispetto dei modelli di gestione e dei requisiti di Qualità definiti nella Convenzione;
- ha una visione complessiva della Convenzione, ne condivide l'andamento con i referenti dell'Amministrazione attraverso incontri periodici, nel Comitato Convenzione, portando in tale

sede proposte migliorative, evidenziando eventuali punti di attenzione e condividendo la strategia di diffusione di tale accordo.

Al **Responsabile Unico del Procedimento** (RUP), lato DTD/Amministrazione aderente, è demandata la titolarità del procedimento e della corretta esecuzione della Convenzione e/o del Contratto di Adesione. La figura incaricata di coordinare i Servizi e di tenere i rapporti con il DEC del DTD e delle Amministrazioni aderenti è rappresentata dal **Direttore del Servizio**. Si configura come *focal point* per l'indirizzo delle scelte strategiche a livello di Governance di progetto. Coordina e dirige le attività del Portfolio Manager, definendo ad alto livello le strategie di allocazione di capacity del costituito RTI. Tra il Direttore del Servizio e il Referente del Servizio c'è un confronto reciproco su informazioni in merito all'andamento della Convenzione, in termini di SLA, raggiungimento degli obiettivi ed eventuali criticità.

Il **Portfolio Manager** è uno specialista nel governo di grandi forniture di servizi per la PA ed ha il compito di **governare e supervisionare** l'andamento dei diversi Contratti d'adesione, nonché di monitorare la conformità dei servizi erogati rispetto agli obiettivi e al budget assegnato. Inoltre, è di sua competenza l'identificazione di criticità a livello macro, connesse alla carenza di personale a livello strutturale, alla inefficace o all'incorretta applicazione dei framework di lavoro a ogni altra problematica di servizio (es. cambi normativi, eventi eccezionali). Il Portfolio Manager è in grado di valutare i rischi potenziali per la fornitura dei CA e di attivare, anche tramite il supporto del Direttore del Servizio, le contromisure necessarie in collaborazione con le altre strutture di governo. È la figura incaricata di coordinare i Servizi di migrazione (DEC - controllo sulla regolare esecuzione della Convenzione in fase di gestione, e alla verifica che le attività e le prestazioni contrattuali siano eseguite in conformità della Convenzione) del DTD e delle Amministrazioni che attivano dei Contratti d'adesione nell'ambito della Convenzione in oggetto.

Al livello di risposta al Contratto di Adesione è previsto un gruppo di Account Team. Ognuno di essi, dedicato al singolo CA, ha in carico le **attività operative** (progetti di migrazione, gestione dei servizi Cliente, etc.) **coordinate dal Technical Team Leader** (TTL – ruolo di supervisione dell'Account Team dal punto di vista tecnico e per gli aspetti legati di esercizio a valle della migrazione, descritto nel capitolo dell'ID 21 cfr. §23) e necessarie per il completamento dei servizi contrattualizzati.

## 19.4 Comitati

La costituzione di Comitati che si riuniscono periodicamente rappresenta un fattore peculiare e distintivo dell'approccio metodologico per la NewCo, il costituito RTI, infatti, considera tali tavoli formali di condivisione fondamentali per una corretta ed ottimale conduzione di programmi complessi, quale la

presente Convenzione. Pertanto, a livello di Convenzione, è prevista la costituzione dei seguenti comitati operativi che saranno organi con funzione di monitoraggio e controllo (e non potere decisionale):

- **COMITATO CONVENZIONE** – Presieduto dal Direttore del Servizio e dal DEC DTD e RUP DTD designati, si occupa del controllo dello stato del programma e dell'avanzamento dei CA. Tale organo, oltre che dalle figure di cui pocanzi, è costituito dal Referente del Servizio. Il comitato può prevedere anche il coinvolgimento di ulteriori figure (legate alle specifiche funzioni di staff – aspetti normativi e legali, sicurezza, impatto CO2, etc.) a supporto del Direttore del Servizio per indirizzare aspetti specialistici legali, normativi, amministrativi, tecnologici, etc. Di particolare rilevanza è quindi il ruolo del Portfolio Manager, che si occupa di supportare il Direttore del Servizio nell'identificare e proporre all'Amministrazione possibili interventi migliorativi nella strategia di comunicazione a favore della diffusione della Convenzione nelle PPAA, trasferendo successivamente tali linee guide alle strutture commerciali della NewCo. Inoltre, la figura di **Enterprise Architect Lead** (EAL), descritta nel Cap. §23 relativo al Criterio ID 21, nel suo ruolo di coordinamento dei Centri di Competenza, attraverso uno scouting continuo, può proporre all'Amministrazione, previa condivisione nel Comitato di Monitoraggio, soluzioni innovative a livello metodologico, tecnologico e di servizio;
- **COMITATO DI MONITORAGGIO** - Presieduto dal Direttore del Servizio, affiancato dal Referente del Servizio, si occupa del monitoraggio di tutti gli aspetti di governo con lo scopo di **uniformare gli approcci e le modalità operative** delle diverse funzioni della società, mantenendo come riferimento unico il modello organizzativo e operativo comune descritto, anche attraverso il supporto della funzione di riferimento (Erogazione Fornitura)**;**

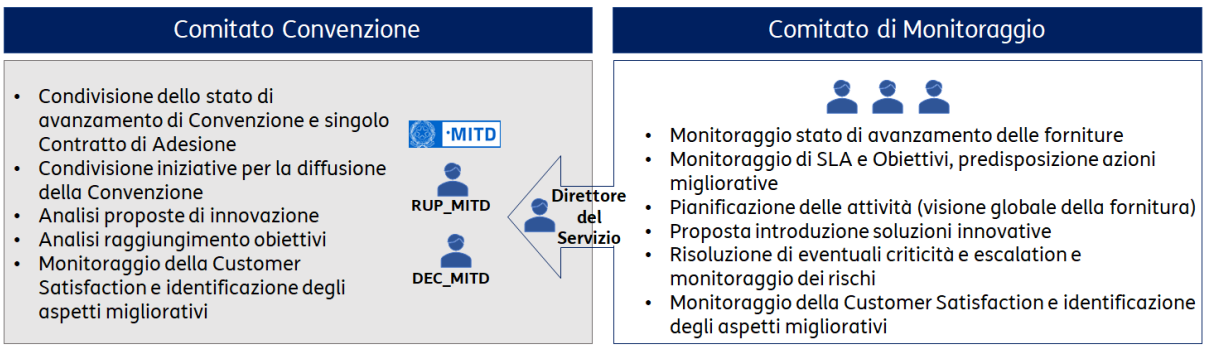



**Figura 12 Comitati a livello di Convenzione**

- **COMITATO DI CONTRATTO DI ADESIONE (CA)** - E' costituito a livello di Portfolio ed è presieduto dal Direttore del Servizio, affiancato dal RUP dell'Amministrazione con il coinvolgimento sia del

DEC che dei Referenti Tecnici della stessa, ha il compito di indirizzare gli aspetti di comunicazione e condivisione dell'andamento della fornitura. Nel Comitato sono inoltre coinvolte le figure di riferimento della fornitura lato NewCo: Portfolio Manager, Transition Manager (TM), il quale, come descritto nel Cap. §23, pianifica e conduce, implementando le linee guida stabilite dal EAL, il progetto di presa in carico dei servizi da parte della struttura operativa della NewCo, il PM di Contratto di Adesione ed i Responsabili delle strutture centrali. Tale Comitato viene riunito, periodicamente o a fronte di particolari esigenze, per condividere lo stato della fornitura con tutti gli attori coinvolti nel governo dei servizi, per monitorare i livelli di servizio contrattuali al fine di individuare eventuali misure correttive/migliorative nell'ottica del Continous Service Improvement.

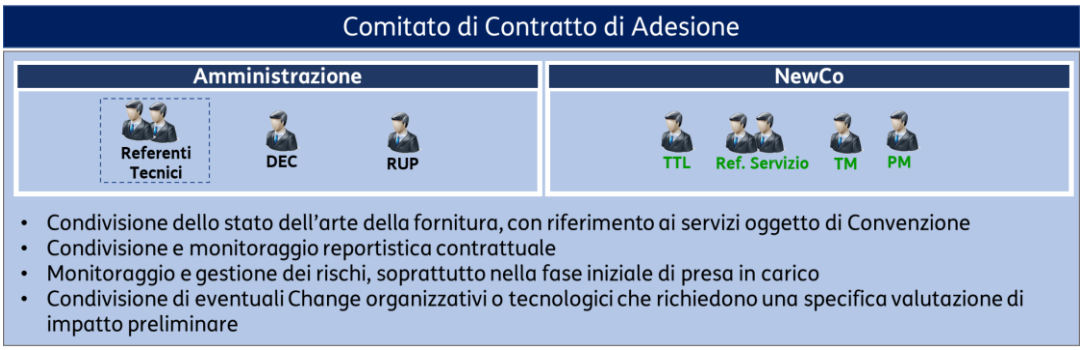



**Figura 13 Comitato di Contratto di Adesione**

I Comitati, costituiti periodicamente, che coadiuvano le funzioni di Governance, precedentemente descritte e presiedute dai Comitati di Convenzione, di Monitoraggio e di CA, sono di seguito descritti:

- **COMITATO DI CONTROLLO** (Trimestrale)- Come previsto dalla Bozza di Convenzione (Allegato 3 sub 6 Bozza di Convenzione con allegati), vigila sull'andamento della Convenzione e può suggerire misure di miglioramento dei Servizi; verifica dell'andamento dei prezzi dei Servizi e degli altri termini ai quali questi sono resi alle Amministrazioni aderenti, in relazione ai prezzi ed alle tecnologie comparabili presenti sul mercato, mantenendo l'equilibrio del Piano Economico Finanziario. E', inoltre, responsabile dell'aggiornamento dei costi e prezzi dell'infrastruttura anche da un punto di vista del refresh tecnologico, come dettagliato nel capitolo relativo al criterio ID 18;
- **COMITATO DI DIREZIONE DELLA FORNITURA** (Semestrale) - Verifica andamento generale e performance complessive del modello di servizio; verifica soddisfazione utenti finali; approvazione e verifica iniziative strategiche; gestione conflitti, violazioni SLA critici e modifiche al modello di servizio; massimo livello di escalation per i temi più critici; valutazione ed

approvazione delle modifiche rilevanti alle consistenze gestite, in accordo con le modalità previste nel processo di gestione delle varianti contrattuali; introduzione e/o dismissione di nuovi servizi;

- **STEERING COMMITTEE** (Mensile) - Gli Steering Committee hanno come obiettivo quello di presentare l'avanzamento complessivo della fornitura e discuterne le problematiche di maggiore rilevanza aventi un impatto a livello di singola Amministrazione aderente, inclusi criticità e rischi (es. vincoli o difformità) grazie al coinvolgimento della funzione di Portfolio Management Office. Alle riunioni, che avvengono con cadenza almeno mensile, prendono parte il Portfolio Manager della classe di Amministrazione aderente in oggetto (es. Pubblica Amministrazione Centrale), il PMCA, la struttura di Portfolio Office, insieme al RUP ed al DEC dell'Amministrazione.

In analogia con quanto proposto a livello di Convenzione, il modello di governance di CA prevede una figura di riferimento unica per l'intera fornitura: il **PM di Contratto Adesione (PMCA)**. Il PMCA:

- costituisce l'interfaccia unica verso l'Amministrazione Aderente per tutti gli aspetti riguardanti l'esecuzione del Contratto e per tutti i servizi contrattualizzati
- rappresenta un punto di coordinamento ed escalation nella definizione di soluzioni e nella gestione di eventuali problematiche/criticità interne al singolo CA;
- fornisce all'Amministrazione reportistica periodica;
- infine, ha il compito di organizzare le attività inerenti alla rilevazione della soddisfazione degli utenti.

Il Referente per la Diffusione della Convenzione (RDC) si impegna a promuovere le novità di carattere sia amministrativo sia tecnico che riguardano la presente Convenzione, proponendosi come punto di contatto tra Amministrazione, Osservatori e le Amministrazioni che aderiscono con singoli CA.

## 19.5 Funzioni di staff

Il Direttore del Servizio e il Referente del Servizio, nell'espletamento delle loro attività, sono coadiuvati da funzioni di staff che forniscono supporto nella gestione contrattuale (Contract management e PMO di Portfolio), della qualità (Quality Auditor), della sicurezza (Risk Management), delle risorse (Resource & Knowledge Management), dell'audit e validazione normativa dell'infrastruttura (Facility Management) e della sicurezza a livello cyber (Organizzazione di Sicurezza). Il Direttore del Servizio e il Referente del Servizio, sulla base delle diverse esigenze, possono richiedere il coinvolgimento di una o più professionalità tra quelle disponibili nelle Funzioni di Staff per indirizzare attività interne specifiche o portare nei Comitati competenze specialistiche, anche a beneficio del DTD o dell'Amministrazione

Aderente. Le risorse appartenenti a tali funzioni sono selezionate tra quelle che possono vantare una consolidata esperienza in contesti analoghi di Convenzioni in ambito Pubblica Amministrazione. La Tabella 2 fornisce una vista di dettaglio delle Funzioni di Staff previste nel modello organizzativo proposto in merito alla funzione di Executive Governance.

*Tabella 2 Funzioni di staff*

| Ruolo | Responsabilità |
|---|---|
| Contract Management | Funzione di supporto per tutti gli aspetti contrattuali. Controlla la corretta esecuzione degli obblighi contrattuali. Svolge attività di verifica della copertura contrattuale e delle performances, identificando, congiuntamente con la funzione di Risk Management, eventuali rischi, valutandoli e fornendo un contributo attivo nell'attribuzione delle priorità di intervento e del piano di mitigazione. Fornisce consulenza alle strutture di produzione nell'interpretazione delle clausole contrattuali. |
| Program Management Office di Portfolio (PMO) | Riferimento per il supporto operativo alle attività di esecuzione dei contratti. Collabora con i PMCA e Referenti di Servizio per rappresentare in un quadro di riferimento unico l'andamento della fornitura in termini di volumi e di impegni. Fornisce consulenza e supporto ai Direttore del Servizio per le attività amministrative della fornitura (es. budget, fatturazione). |
| Quality Auditor | Riferimento unico per tutti gli aspetti legati alla qualità. È responsabile, per ogni CA, del Piano di Qualità del progetto di fornitura e lo modifica a fronte delle richieste dell'Amministrazione. Esegue e coordina le verifiche di qualità secondo i piani approvati. Supporta l'Amministrazione nelle verifiche ispettive sulla fornitura. Supporta il RUP DTD e il Referente del Servizio nell'analisi dei dati relativi a SLA, rilievi e penali e concorda azioni di mitigazione con il TTL e le strutture operative. |
| Resource & Knowledge Management | Riferimento per gli aspetti di selezione delle risorse professionali per lo svolgimento dei servizi. Identifica, congiuntamente con il TTL e con le strutture operative della NewCo, i requisiti della fornitura in termini di risorse e profili professionali. Mantiene uno skill inventory delle risorse e definisce il piano di formazione e certificazione. Collabora sia con i responsabili delle strutture |

| | |
|---|---|
| | operative, sia con i Referenti dei servizi per l'aggiornamento continuo del Piano delle Risorse sulla base delle esigenze. |
| Risk Management | Supporta l'intera organizzazione della NewCo in tutti gli aspetti di valutazione del rischio, analizzando e applicando la matrice di ripartizione del rischio, proposta nel criterio ID 16 di cui al Disciplinare di gara. Questa funzione è importante sia per la verifica periodica degli aspetti operativi dei servizi forniti rispetto alla tematica del rischio, sia in fase di presa in carico dei servizi, congiuntamente al TM, per valutare e mitigare tutti i rischi connessi all'attivazione ed erogazione dei nuovi servizi da parte della NewCo. |
| Facility Management | Interviene nell'auditing e nella validazione della corretta rispondenza dell'infrastruttura e ai servizi alle normative vigenti e alle Determine emesse da Enti quali, ad es., AgID o ANC. |
| ESG Performance Management | Riferimento unico per tutti gli aspetti legati ai criteri di ESG. È responsabile della pianificazione e del monitoraggio del rispetto di aderenza al quadro normativo di riferimento (Rif. Criterio ID 15). È responsabile dell'implementazione e della gestione del piano di sostenibilità. |
| Organizzazione di Sicurezza | Si occupa, in aderenza alle normative di riferimento, di indirizzare gli aspetti di sicurezza cibernetica della fornitura, monitorandoli sui singoli CA ed a livello complessivo di Convenzione per tutta la durata contrattuale. Si rimanda al capitolo relativo al Criterio ID 19 per il dettaglio. |
| Help Desk | E' il punto unico di contatto tra le Amministrazioni aderenti e le strutture operative della NewCo, si interfaccia in modalità multicanale (fax, mail, telefono, web) sia con i Referenti sia con gli utenti dell'Amministrazione aderente. Tale struttura è articolata su due livelli:<br>- Help Desk I Livello – Tale gruppo, utilizzando gli strumenti previsti dal Capitolato per l'erogazione dei servizi, effettua attività di ricezione delle segnalazioni, tipizzazione ed apertura ticket;<br>- Help Desk II Livello – Tale gruppo si occupa della risoluzione delle segnalazioni non risolte dall'Help Desk di I° livello, contattando, se necessario, l'utente sulla base delle priorità assegnate. |

| | |
|---|---|
| Service Manager | Gestisce e coordina le attività a livello di singolo CA e pianifica i singoli interventi sulla base dei seguenti elementi:<br>• Livello di servizio da garantire;<br>• Disponibilità del servizio della PA su cui effettuare l'intervento;<br>• Monitoraggio degli interventi pianificati. |

## 19.6 Piano di comunicazione

Allo scopo di ottimizzare l'efficacia delle strutture di governance ed operative nel contesto delle Amministrazioni, in fase di avviamento di Convenzione e dei singoli CA, la NewCo si occupa di:

- identificare tutti gli stakeholder del progetto e le organizzazioni/strutture di cui fanno parte;
- definire quali comunicazioni devono essere scambiate tra gli stakeholder durante l'intero ciclo di vita del programma/progetto, assicurando che tutti essi siano adeguatamente informati e coinvolti nella modalità più appropriata;

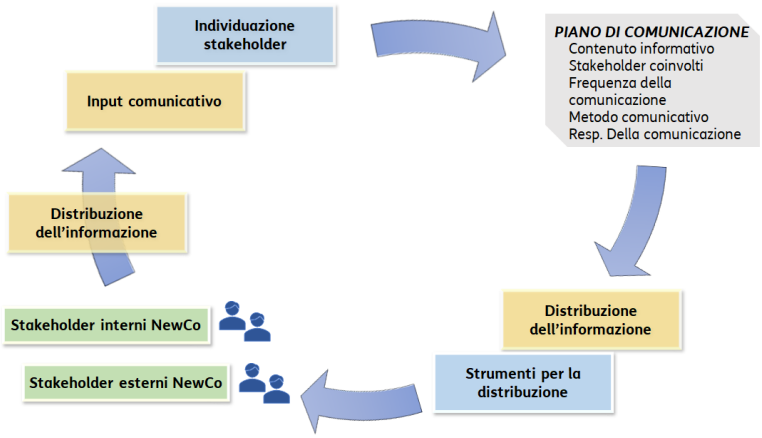



**Figura 14 Piano di comunicazione**

- fornire informazioni chiare, consistenti ed accessibili a tutti gli attori coinvolti, assicurando che le opinioni ed i punti di vista siano tenuti nella giusta considerazione.

Il processo di gestione dei flussi di comunicazione, i cui principali destinatari di questo flusso informativo sono il Concedente e le singole Amministrazioni Aderenti, ha l'obiettivo di assicurare una tempestiva e adeguata produzione, raccolta, distribuzione, archiviazione e consultazione di tutte le informazioni necessarie all'erogazione della fornitura.

Ciò si traduce in una preventiva pianificazione delle azioni comunicative da attuare a fronte di ciascun input comunicativo, quali ad esempio Piano di lavoro periodico, informazioni sui ticket, relazioni sui Livelli di Servizio.

Il Piano di comunicazione definisce, pertanto, le esigenze informative che devono essere soddisfatte per gli stakeholder: chi è il destinatario delle informazioni, quando è previsto l'inoltro, come vengono fornite le informazioni e da chi. La responsabilità della predisposizione e gestione di tale piano è a carico delle

Funzioni di Governo della Fornitura (RUP dell'Amministrazione e Direttore del Servizio, supportati dalle Funzioni di Staff, in particolare dal PMO di Portfolio e dall'EAL). Di seguito si riporta uno schema illustrativo delle interazioni tra le figure di riferimento della NewCo e quelle della singola PA in fase di CA.

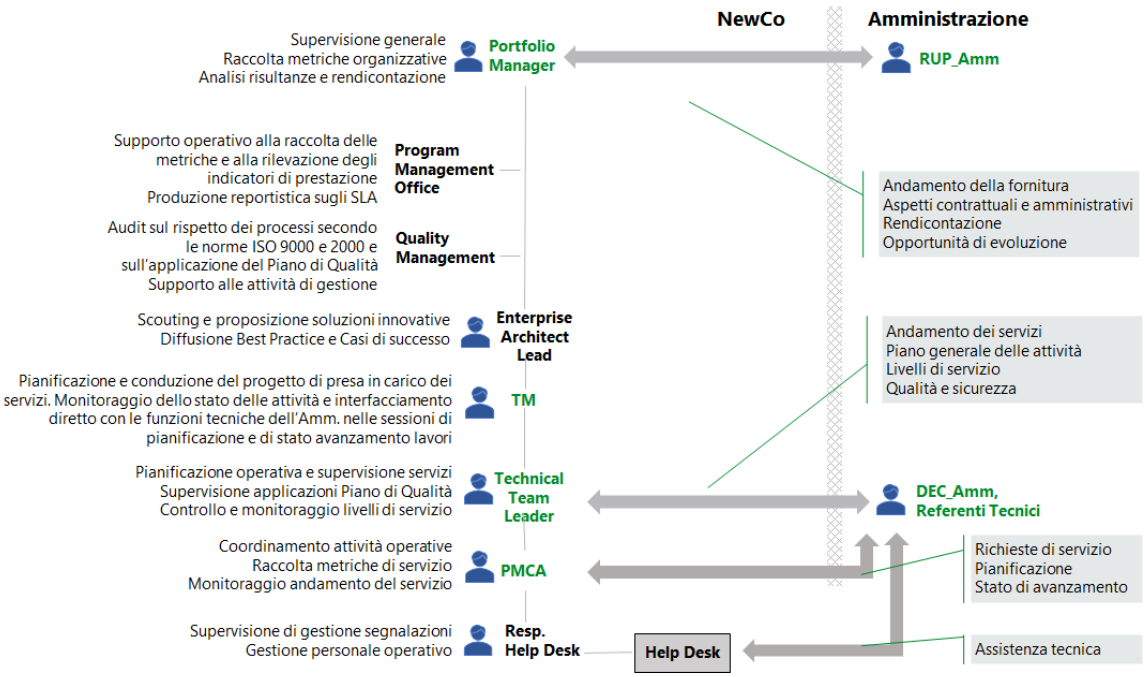



**Figura 15 Piano di Comunicazione**

A tal proposito, vengono identificati, in accordo con la committenza (Il DTD per la Convenzione, le singole Amministrazioni per i CA):

- i principali stakeholder;
- le organizzazioni che hanno un impatto diretto o indiretto sul programma e sui singoli CA;
- la tipologia di incontri periodici;
- il flusso della comunicazione (in ambito dei singoli CA e del programma globale).

A livello organizzativo, l'efficacia delle interazioni e dei flussi di informazione è garantita da:

- responsabilità chiare;
- compiti operativi noti e condivisi;
- periodicità stabilita per la diffusione delle informazioni;
- preventiva definizione delle modalità operative per la diffusione delle informazioni.

Inoltre, l'efficienza delle comunicazioni è assicurata mediante la disponibilità di strumenti per la distribuzione delle informazioni che garantiscano sia la tempestività nella diffusione, in caso di eventi inattesi, sia la persistenza, alimentando la knowledge base di fornitura, ovvero:

- portale di fornitura per la condivisione delle informazioni (piani di lavoro, stati avanzamento lavoro, rapporti di sintesi e di dettaglio, etc.);
- knowledge base, quale strumento per la condivisione della conoscenza tra i gruppi di lavoro (lesson learned).

Il Piano di comunicazione è definito in fase di avvio della fornitura ed i risultati sono periodicamente esaminati nel corso della durata contrattuale, provvedendo eventualmente, a revisionarlo o integrarlo al fine di garantirne l'applicabilità.

I principali flussi informativi interni all'organizzazione proposta sono:

- governo convenzione → erogazione della fornitura: al fine di diffondere linee guida, comportamenti e procedure da adottare nell'erogazione dei Servizi;
- erogazione della fornitura → governo convenzione: per segnalare eventi significativi emersi nell'ambito dell'erogazione dei Servizi;
- erogazione della fornitura → erogazione della fornitura: per la diffusione della conoscenza nell'ambito dei processi di knowledge management.

Ai flussi sopra indicati si affiancano tutte le comunicazioni previste verso il Concedente e ciascuna Amministrazione aderente.

## 19.7 Processi / Interazioni con il Concedente e ciascuna Amministrazione aderente e con i Fornitori Terzi

Per una visione complessiva del modello organizzativo, si riporta, nella seguente figura, il dettaglio dei **Macro-Processi Operativi di Governance e di Service Delivery & Operations**.

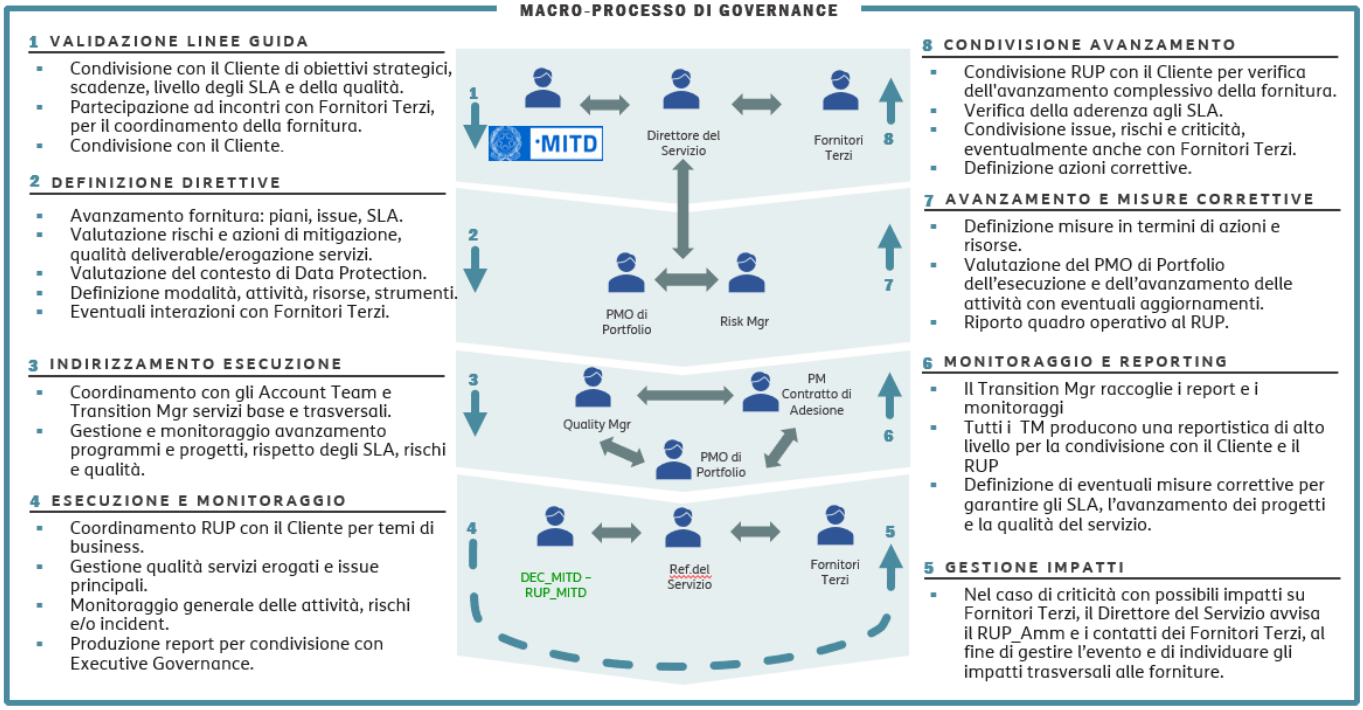



**Figura 16 Macro-processo di Governance**

I confronti previsti tra le figure di responsabilità della NewCo ed i relativi riferimenti del DTD sono funzionali ad allineare L'avanzamento della fornitura con gli obiettivi del DTD. Tali confronti, inoltre, assicurano una costante condivisione delle strategie e delle modalità operative, consentendo il monitoraggio continuo dell'avanzamento della Convenzione ed il controllo del raggiungimento degli SLA.

Con l'obiettivo di rendere più efficace la gestione dei task di interesse del DTD, quali ad esempio la risoluzione di fault critici o massivi sull'infrastruttura, la predisposizione di offerte a progetto e la gestione di ritardi nelle pianificazioni con possibili impatti sul Business, la NewCo inserisce nel proprio modello operativo un **processo di escalation strutturato,** attivabile dal DTD in caso di particolari eventi o criticità. Il punto di ingresso di tale processo è rappresentato dal PMO di Portfolio, che ha responsabilità in queste particolari situazioni di attivare con la corretta priorità le risorse della NewCo, al fine di risolvere con tempestività gli eventi e/o le situazioni critiche. Nella tabella sottostante sono riportati i "checkpoint" proposti.

*Tabella 3 Checkpoint - Frequenza*

| Checkpoint (frequenza) | Attività/obiettivi principali | partecipanti |
|---|---|---|

| | | |
|---|---|---|
| **SAL Service Management (Mensile)** | Incontro di condivisione periodica per la verifica dell'avanzamento complessivo della fornitura; valutazione della qualità dei servizi, degli SLA, e delle penali; gestione escalation e criticità; condivisione principali azioni correttive/preventive. | Direttore del Servizio, Referente del Servizio, DEC DTD, RUP DTD |
| **Meeting Innovation (Trimestrale)** | Incontro di condivisione delle analisi dei trend di innovazione e di evoluzione digitale; definizione e aggiornamento degli obiettivi di innovazione e trasformazione digitale. | EAL, Referente del Servizio, RUP DTD |
| **SAL di Gestione (Trimestrale)** | Incontro di condivisione periodica per la verifica dell'andamento degli Account Team; analisi attività (pianificazione task, allocazione risorse, etc.) e qualità dei servizi; gestione problemi e criticità; azioni correttive/preventive. | Portfolio Manager, Direttore del Servizio, DEC DTD, Service Manager |
| **Meeting di Data Protection (Quadrimestrale)** | Incontro di allineamento per verifica degli impatti (DPIA); adeguamenti al Garante Privacy o alle autorità giudiziarie; rilevazione delle criticità e identificazione delle azioni correttive/preventive; modifiche e/o aggiornamenti del framework di Data Protection. | Direttore del Servizio, Referente del Servizio, RUP DTD, DEC DTD, DPO |

Sono inoltre previsti dei momenti di confronto con i Fornitori Terzi, funzionali a: condividere gli indirizzi su tematiche legate alla migrazione end-to-end; assicurare la coerenza nella conduzione dei servizi rispetto alle indicazioni e alle strategie definite dall'Amministrazione; garantire coerenza degli interventi con l'evoluzione complessiva dei sistemi e dei servizi; assicurare una costante condivisione degli obiettivi e delle modalità operative implementate; garantire la condivisione sistematica dei problemi rilevati.

*Tabella 4 Checkpoint aggiuntivi - Frequenza*

| Checkpoint (frequenza) | Attività/obiettivi principali | Partecipanti |
|---|---|---|
| **Ecosystem Strategic Review (Annuale)** | Condivisione andamento dei servizi e performance dell'eco-sistema; verifica soddisfazione utenti finali; gestione iniziative strategiche ed azioni di evoluzione e miglioramento servizi; allineamento Fornitori alle priorità e alle strategie della NewCo; comitato di coordinamento strategico sulle tematiche di innovazione. | Direttore del Servizio, Referente del Servizio, DEC DTD, RUP DTD, Portfolio Manager |
| **IT Executive Review (Trimestrale)** | Valutazione delle performance end-to-end; revisione financials/spending e valutazione eccezioni; proposte evoluzione e miglioramento; revisione rischi e criticità evidenziati dal PMO; valutazione livello soddisfazione utenti; analisi retrospettive degli eventi significativi. | PMCA, Portfolio Manager, Referente del Servizio, RUP DTD |
| **Integrated Service Review (Bisettimanale/ Mensile)** | Supervisione attività di implementazione ed erogazione dei servizi in ottica end-to-end; garanzia dell'integrazione dei Fornitori secondo il modello multi-sourcing; proposte di evoluzioni architetturali; valutazione iniziative strategiche integrate; analisi retrospettive e azioni di miglioramento; follow-up azioni integrate. | PMCA, Portfolio Manager, Referente del Servizio, RUP DTD |
| **Gestione delle criticità minori (Bisettimanale)** | Condivisione di issue a bassa/media criticità, con possibili impatti su altre forniture; coordinamento nella definizione degli interventi di gestione degli stessi; identificazione delle possibili sinergie e pianificazione del piano di *Remediation*. | Portfolio Manager, PMCA per singola Amministrazione aderente |

| | | |
|---|---|---|
| **ESG Reporting Review (Semestrale)** | Condivisione di livelli di performance raggiunti nell'ottica del soddisfacimento dei parametri relativi alle linee guida interne e alla normativa di riferimento. Si rimanda alla descrizione del criterio ID 15, in cui si evidenzia, inoltre la messa a disposizione di un report derivante da un tool per il monitoraggio dell'impatto ambientale legato alla fornitura dei servizi (Carbon Footprint Calculator). | Direttore del Servizio, Referente del Servizio, DEC DTD, RUP DTD, Portfolio Manager |

## 19.8 Strumenti a supporto dell'organizzazione

Lo strumento principale di condivisione delle informazioni è il Portale della fornitura, tramite il quale vengono condivise tutte le informazioni necessarie a garantire la massima trasparenza ed il corretto monitoraggio pubblico, ad esempio la reportistica sullo stato della Convenzione in merito alle adesioni, al budget disponibile, ai verbali relativi ai checkpoint descritti al par. 19.7.

Nello specifico il Portale della Fornitura prevederà:

1. accesso, tramite account online dedicato, del Responsabile Unico di Progetto (RUP) e dei membri del Comitato di Controllo alle Aree "Collaborazione e Monitoraggio" e "Osservatori" del portale web al fine di garantire il monitoraggio e la *governance* diretta ed in tempo reale della Convenzione;
2. integrazione, addizionalmente rispetto alle informazioni già previste, della dashboard nell'Area "Collaborazione e Monitoraggio" con funzionalità di reportistica che consenta una visione d'insieme *real time* dello stato di avanzamento dei lavori con i seguenti indicatori:
    - numero di Pubbliche Amministrazioni per fase di adesione al PSN (i.e. …, definizione del piano dei fabbisogni, in corso di migrazione, migrazione completata) in valore assoluto e in comparazione rispetto al target di piano;
    - volume complessivo di servizi acquistati dal PSN con relativa spesa impegnata in valore assoluto e in comparazione rispetto al target di piano;
    - distribuzione dei servizi acquistati dalle PA tra i servizi offerti a catalogo in valore assoluto e in comparazione rispetto al target di piano.

3. integrazione, addizionalmente rispetto alle informazioni già previste, della dashboard nell'Area "Collaborazione e Monitoraggio" con dati che consentano non solo il monitoraggio e il controllo ma anche la valutazione degli impatti del livello di adesione dei progetti in corso di realizzazione. In particolare, la dashboard verrà integrata con le seguenti informazioni[1]:
    - indicatori sintetici dei consumi energetici post adesione al PSN e risparmio rispetto alle soluzioni precedentemente adottate dalle Pubbliche Amministrazioni clienti del PSN;
    - indicatori relativi agli impatti ESG derivanti da:
        - risparmio energetico e sfruttamento di energia generata da fonti rinnovabili (es. riduzione quantità CO2 emessa, % energia rinnovabile su totale consumo energia);
        - inclusione e soddisfazione sul posto di lavoro (es. % giovani, % donne, % assenteismo, % turnover, eNPS, presenza di codici di condotta interni);
        - impatto sulla comunità e formazione della forza lavoro (es. importi speso a supporto della comunità locale, ore di formazione / dipendente / anno).
    - stima del risparmio complessivo di spesa pubblica da parte delle PA aderenti ottenuto dall'implementazione dei progetti realizzati;
    - indicatori sintetici dell'incremento negli indici di sicurezza e riduzione del rischio di down time dei server rispetto alle soluzioni precedentemente adottate dalle Pubbliche Amministrazioni clienti del PSN;
    - indicatori di Cybersecurity (e.g. numero di eventi di sicurezza per categoria, numero di incidenti, vulnerabilità sui sistemi, etc.);
4. previsione di un report annuale integrato, comprendente informazioni finanziarie e non finanziarie, al fine di dare una visione d'insieme rispetto alla strategia, modello operativo e governance della NewCo, ovvero la sua capacità di creare nel tempo valore sostenibile a favore dei propri stakeholder. Nello specifico, il reporting non finanziario sarà redatto in conformità alle metodologie e ai principi previsti dai GRI Sustainability Reporting Standards pubblicati dal Global Reporting Initiative ed includerà, tra gli altri, una serie di indicatori coerenti con i criteri tabellari e valutativi richiesti e descritti nel disciplinare di gara, anche al fine di garantire ulteriormente all'Amministrazione Concedente la vigilanza e il monitoraggio pubblico;
5. creazione di una apposita sezione nell'Area "Collaborazione e Monitoraggio" per il monitoraggio dell'implementazione delle iniziative del PNRR relative al PSN, con particolare riferimento

[1] I dati verranno pubblicati in base alla disponibilità delle Pubbliche Amministrazioni aderenti al PSN alla condivisione e pubblicazione in via anonima e aggregata degli stessi relativamente alle informazioni riguardanti lo status preadesione PSN

all'ammontare dei fondi PNRR erogati alle Pubbliche Amministrazioni aderenti al PSN rispetto ai target e milestone previsti dagli Investimenti 1.1 e 1.2 della M1C1;

6. integrazione dell'ambiente telematico social previsto nell'Area "Collaborazione e Monitoraggio" con un'area di interazione dedicata alle Pubbliche Amministrazioni clienti del PSN per (i) fornire al PSN sia in via anonima che in via pubblica le istanze delle Amministrazioni stesse al fine di integrare e prevedere, ove necessario, miglioramenti alle caratteristiche dei servizi e alla gestione dell'infrastruttura, nonché ad ogni altro aspetto che possa influenzare positivamente la qualità dell'offerta PSN e (ii) avere la possibilità di scambiare esperienze e/o suggerimenti con altre Amministrazioni utenti;
7. integrazione del portale della fornitura nell'Area "Collaborazione e Monitoraggio" con un'ambiente di monitoraggio a livello di Convenzione, il *Masterplan di Convenzione*, che riporta, in maniera cumulativa, le iniziative in corso di esecuzione. Saranno evidenziati: pianificazione temporale dei task, stato di avanzamento, owner, milestone, deliverable, economics associati, criticità, azioni di rientro proposte, nonché informazioni su eventuali non conformità e/o mancate accettazioni del servizio/prodotto;
8. creazione di un'ambiente, nell'Area di "Collaborazione e Monitoraggio", *Monitoraggio KPI di Convenzione*, al fine di monitorare i KPI al fine di gestire l'andamento dell'intera Convenzione.

Di seguito, a corredo dei KPI relativi all'erogazione del servizio descritti nel capitolo 23 relativo al criterio ID 21, vengono presentati, a titolo esemplificativo e non esaustivo, i KPI relativi al governo della fornitura. Tali KPI potranno essere categorizzati a seconda del livello di complessità del progetto di migrazione secondo i criteri evidenziati nel capitolo 22 relativo al criterio ID 20.

### KPI01 - Backlog Contratti di Adesione

| | |
|---|---|
| Parametro | Adesione alla Convenzione |
| Elemento valutativo | Amministrazioni che hanno aderito effettivamente alla Convenzione |
| Unità di misura | Percentuale |
| Periodo di misura | Anno |
| Grandezze | Numero di Amministrazioni che hanno aderito alla convenzione [*NAmAD*] e Numero Amministrazioni Totali [*NAmTOT*] |
| Formula | $\frac{NAmAD}{NAmTOT}$ |

### KPI02: Impegno Portfolio

| | |
|---|---|
| Parametro | Budget consumato associato al portafoglio |
| Elemento valutativo | Valore economico Contratti di Adesione |
| Unità di misura | Percentuale |
| Periodo di misura | Anno |
| Grandezze | Valore economico Contratti d'Adesione [*VeCA*] e Budget annuo Portafoglio [*BaP*] |
| Formula | $\frac{VeCA}{BaP}$ |

### KPI03: Progetti di Migrazione

| | |
|---|---|
| Parametro | Progetti di Migrazione Attivati |
| Elemento valutativo | Numero di Progetti attivati dalle amministrazioni |
| Unità di misura | Valore assoluto |
| Periodo di misura | Anno |
| Grandezze | Numero di Progetti Attivati [*NPA*] |
| Formula | $\sum Pa$ |

### KPI04: Backlog Progetti

| | |
|---|---|
| Parametro | Progetti di Migrazione effettivamente conclusi |
| Elemento valutativo | Numero di Progetti di migrazione conclusi |
| Unità di misura | Percentuale |

| | |
|---|---|
| Periodo di misura | Anno |
| Grandezze | Numero di Progetti Conclusi [*NPC*] e Numero di Progetti Attivati [*NPA*] |
| Formula | $\frac{NPC}{NPA}$ |

### KPI05: Durata Media Progetti

| | |
|---|---|
| Parametro | Durata media progetto di migrazione |
| Elemento valutativo | Tempistiche migrazione |
| Unità di misura | Working day |
| Periodo di misura | Anno |
| Grandezze | Durata Complessiva Progetti [*DCP*] e Numero Progetti Conclusi [*NPC*] |
| Formula | $\frac{DCP}{NPC}$ |

### KPI06: Ritardo consegna Progetti

| | |
|---|---|
| Parametro | Ritardo medio conclusione progetto di migrazione |
| Elemento valutativo | Tempistiche migrazione |
| Unità di misura | Working day |
| Periodo di misura | Anno |
| Grandezze | Durata Stimata Progetti [*DSP*] Durata Complessiva Progetto [*DCP*] |
| Formula | $\frac{DSP}{DCP}$ |

Pertanto, il portale arricchito dalle funzionalità precedentemente esposte, oltre che garantire la corretta e completa gestione dei servizi professionali tecnici, può esser visto come una "piazza" nella quale il DTD, le Amministrazioni Aderenti, gli Osservatori e la NewCo si "incontrano" per discutere di specifiche tematiche che possono essere di interesse. In particolare, il Portale risulta particolarmente utile al RDC, che può facilmente consultare tutti i report e i dati statistici relativi all'andamento generale della Convenzione, in primo luogo quelli relativi ai KPI precedentemente descritti.

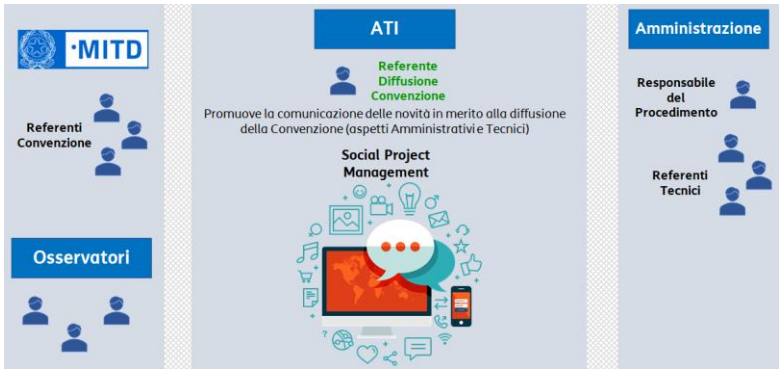



**Figura 17 Attori coinvolti**

Il Portale apporta quindi numerosi vantaggi, sia in termini di tecniche di comunicazione digitale e tradizionale, che di carattere tecnologico grazie alle funzionalità specifiche degli strumenti utilizzati, che vengono evidenziati nella tabella seguente:

*Tabella 5 Vantaggi del portale*

| Vantaggio | Descrizione | Stakeholder coinvolti |
|---|---|---|
| Digitali | Supporto alla creazione di una "data room" composta da membri di alto profilo in grado di monitorare costantemente le discussioni online e offline, di capire le dinamiche e i "nodi" strategici per la comunicazione degli obiettivi comuni del servizio proposto, intervenire in caso di problemi (flame o crisi conclamate), guidare le attività di comunicazione in ottica "data driven" | Amministrazione, Istituzioni Pubbliche, NewCo |
| | Realizzazione di comunicati stampa su account social. | Digital Marketing Expert |
| Tradizionali | Rafforzamento dei presidi di relazioni con i media – online e offline – con particolare attenzione ai portali generalisti. Le eccellenze del sistema italiano potranno essere anche | Amministrazione, NewCo, Amm.ni Aderenti |

| | | |
|---|---|---|
| | veicolate alla stampa estera, con cui effettuare appositi incontri | |
| | Consulenza alla realizzazione di un web magazine dall'elevato contenuto autoriale, che diventi il punto di riferimento delle opportunità offerte dalla Convenzione. Il magazine potrà ospitare interventi di opinion leader/maker per rafforzare i legami tra gli stakeholder e potrà essere affiancato da una newsletter | Amministrazione, NewCo, Amm.ni Aderenti, PMO |
| | Supporto all'identificazione e alla partecipazione a eventi coerenti con il posizionamento degli obiettivi della Convenzione (es. Maker Faire) | DTD, NewCo, Amm.ni Aderenti, Digital Marketing Expert |
| Tecnologici | Portale completamente integrato basato su un'unica base dati per facilitare la consultazione, lo scambio rapido e sicuro dei dati e l'elaborazione e creazione anche in autonomia della reportistica desiderata | Amministrazione, NewCo, Amm.ni Aderenti, PMO, Osservatori |
| | Il Portale metterà a disposizione di tutti gli utilizzatori interni (NewCo) ed esterni (PA/Osservatori) un social enterprise networking che consente scambio di informazioni e documenti, nel pieno e totale rispetto della privacy | Amm.ni Aderenti, PMO, Osservatori, Amministrazione, NewCo |
| | Utilizzo di tecniche di SEO (Search Engine Optimization) volte a migliorare il posizionamento nei motori di ricerca a fronte di possibili parole chiave utilizzate dalle Amministrazioni (esempio Convenzione, Servizi Cloud IaaS e PaaS) | Amministrazione, NewCo, Amm.ni Aderenti |

Inoltre, la NewCo, al fine del corretto monitoraggio dei dati all'interno dei DC e a supporto dei servizi forniti di Industry Standard, adotta un innovativo paradigma del "**Digital Twin"** di accesso e visualizzazione dei dati. La visualizzazione dei dati con una rappresentazione grafica sovrapponibile a ciò che si trova fisicamente on site annulla lo sforzo interpretativo, velocizzando i processi e semplificando analisi e ricerche. Il sistema consente all'Amministrazione di navigare virtualmente tra gli apparati, come se si trovasse realmente in sala. Il confronto visivo tra virtuale e reale permette di

evidenziare e correggere immediatamente eventuali discrepanze, aumentando notevolmente la qualità del dato.

Per il monitoraggio delle server room e degli asset nel DC è quindi previsto l'utilizzo di uno **strumento innovativo** denominato ALE (Advanced Live Environment) che permette di rappresentare i dati in Virtual Reality: la replica virtuale degli elementi del Data Center permette di interagire remotamente in maniera completa, eseguire ispezioni visive, fornire indicazioni puntuali al personale in loco per disporre gli interventi richiesti.

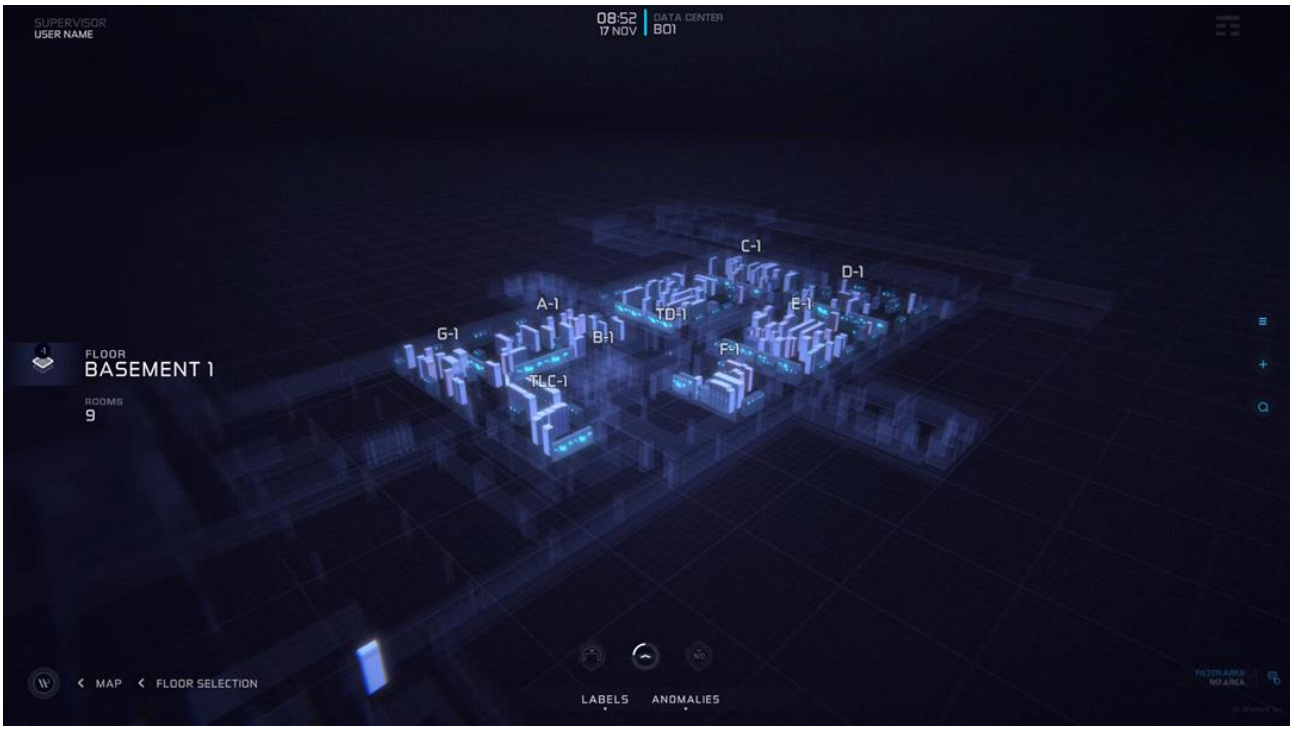



**Figura 18 Esempio di vista Data Center**

Il sistema permette la visualizzazione delle seguenti viste di navigazione, a titolo esemplificativo e non esaustivo:

- vista mappa: visualizza la cartina con tutti i Data Center da cui saranno erogati i servizi del PSN;




**Figura 19 Esempio vista Mappa**

- vista Data Center: in questa vista si vedono i piani di cui è composto il DC, con una prima rappresentazione dei rack nelle sale; i rack che contengono anomalie sui dati sono evidenziati da colore rosso;
- vista Floor: in questa vista vengono evidenziate tutte le sale del piano con i relativi rack;
- vista Room: in questa vista i fianchi dei rack spariscono evidenziandone il contenuto. La selezione di un rack (singolo tap/click) visualizza sui pannelli informativi di sinistra le relative informazioni;
- vista Rack: in questa vista sono riportati i dati del rack stesso e dei singoli apparati dentro il rack;
- vista Connessioni fisiche e logiche.

# 20 ID 18 – Valutativo - Miglioramenti, a favore del Concedente, della compliance nell'aggiornamento dei costi e prezzi dell'infrastruttura anche da un punto di vista del refresh tecnologico. Tali miglioramenti, per essere apprezzati, devono essere chiari, evidenti e, possibilmente, misurabili

## 20.1 Executive summary

Il Costituito RTI, in relazione alla premialità legata ai miglioramenti sugli aspetti di aggiornamento prezzi, elabora una proposta di Convenzione derivante dall'esperienza maturata nella gestione di grandi Contratti Quadro per i quali è stato implementato con successo un meccanismo di adeguamento dei prezzi all'interno di un processo ampio, strutturato e consolidato e prevede all'art.30 di operare eventuali varianti nel rispetto dei limiti dell'articolo 175 del Codice degli Appalti.

In questo capitolo sarà illustrata la metodologia che permette di evidenziare il miglioramento che si propone rispetto a quanto già previsto nella bozza di convenzione: nel § 20.2 sarà descritto il sistema di verifica messo a punto dal costituito RTI che tiene conto del refresh tecnologico e dell'evoluzione degli standard tecnici e che utilizza un insieme di processi in grado di realizzare le attività di controllo necessarie a valutare le modalità di aggiornamento dei costi; nel § 20.3 sono mostrate le modalità operative che consentono di giungere ad una definizione condivisa dell'aggiornamento dei prezzi.

Infatti, la proposta del costituito RTI prevede che, successivamente alla sottoscrizione della Concessione, come già riportato e descritto nell'articolo 12 del documento di gara *Allegato 3 - sub 6 – Bozza di Convenzione con Allegati*, sia costituito un organismo tecnico di coordinamento e governo denominato **Comitato di Controllo (CdC)**, formato da membri del Concedente e del Concessionario oltre che da rappresentanti indipendenti, di comprovata esperienza sul tema specifico, candidati da soggetti istituzionali quali ad esempio AgID o da equivalenti enti/organi pubblici o partecipati: questi nominativi saranno valutati dallo stesso CdC che potrà formalizzare la loro nomina come membri in carica dello stesso Comitato, in accordo con le regole che lo stesso avrà definito.

Come proposto all'articolo 5 comma 4 della sopra citata bozza di Convenzione, tra i compiti del **CdC** rientra l'attività di valutare il contenuto dei servizi, sia dal punto di vista qualitativo (aggiornamento dei servizi con l'uso di nuove tecnologie) sia economico, attraverso i meccanismi di valutazione dei costi che di adeguamento dei prezzi. Per quest'ultima attività il CdC svolgerà periodicamente, in autonomia o tramite terzi, un'approfondita indagine atta a rilevare i migliori prezzi di mercato di servizi analoghi a quelli erogati nell'ambito dei Contratti di adesione. L'analisi dei benchmark così svolta, eventualmente con il supporto di società terze con esperienza nel settore, dovrà essere ispirata ai principi descritti nel §20.3. In analogia a quanto previsto per l'aggiornamento dei prezzi, la NewCo si impegna ad effettuare approfondite analisi di mercato al fine di valutare ed adeguare i costi e le tecnologie utilizzate nell'ambito della Convenzione.

Con riferimento alle tempistiche riportate nell'articolo 5 comma 4 già citato, la NewCo si impegna ad aggiornare i prezzi unitari per i vari contratti di adesione a partire dal terzo anno dalla stipula della Convenzione, al termine della finestra di adesione, pari a 30 mesi, delle Amministrazioni; tale adeguamento avverrà con frequenza pari a 24 mesi.

Nel diagramma di flusso che segue (Figura 20) si descrive il processo di interazione tra CdC e NewCo finalizzato alle attività di adeguamento costi, refresh tecnologico e prezzi descritti nei paragrafi a seguire.

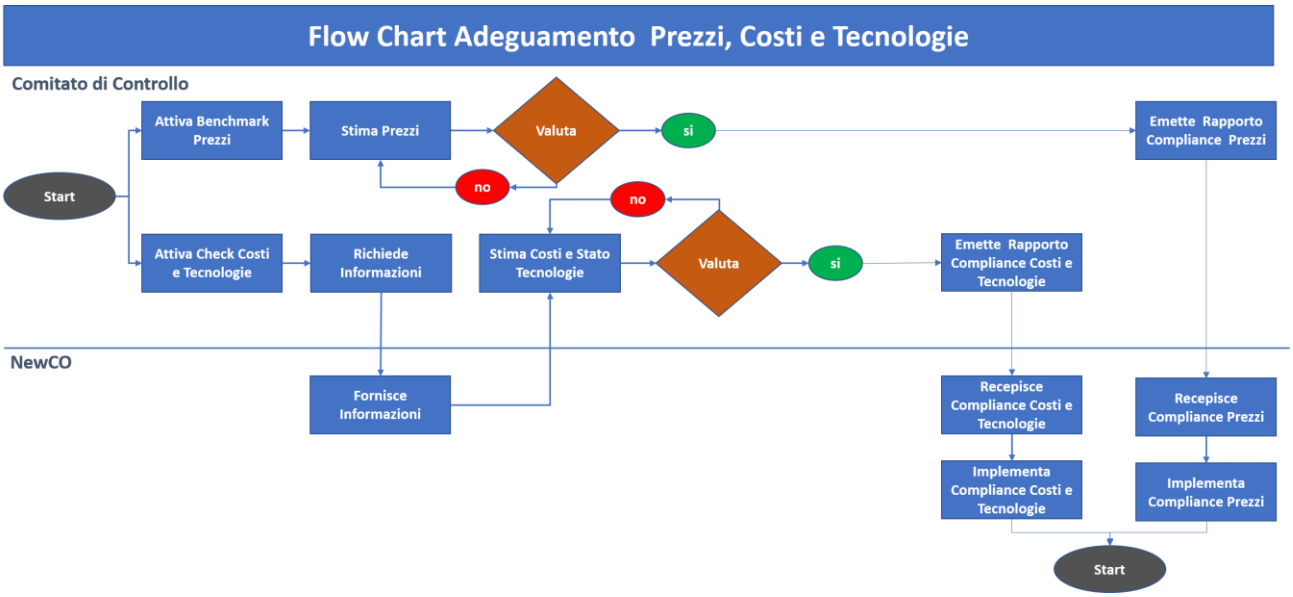



**Figura 20 Processo di adeguamento prezzi, costi e tecnologie**

## 20.2 Modalità operative per il controllo dei costi ed il refresh tecnologico

Tenendo anche conto del refresh tecnologico necessario nel periodo della Convenzione, per migliorare la compliance nella valutazione dei costi del PSN, sono state identificate delle strategie e dei KPI interni che permettono di mantenerli in linea alle effettive necessità di servizio.

Come rappresentato in Figura 21, i check identificati forniscono un input al CdC per le azioni che rientrano nei suoi compiti, come ad esempio la rideterminazione del contenuto dei servizi offerti dal PSN e dei costi ad essi associati.

Le linee di azione sono:

- **la verifica dei servizi acquisiti** dalle singole amministrazioni, con l'intento di identificare quali sono le reali necessità delle stesse in relazione ai servizi del PSN, evidenziando anche quelli non necessari, ovvero "poco efficaci" – **effectiveness check**. Questo permette una ottimizzazione dei costi, realizzando risparmi sia attraverso la riduzione della disponibilità di capacità elaborativa per servizi a bassa (o nulla) richiesta, sia mettendo a disposizione quelli più richiesti a costi inferiori;

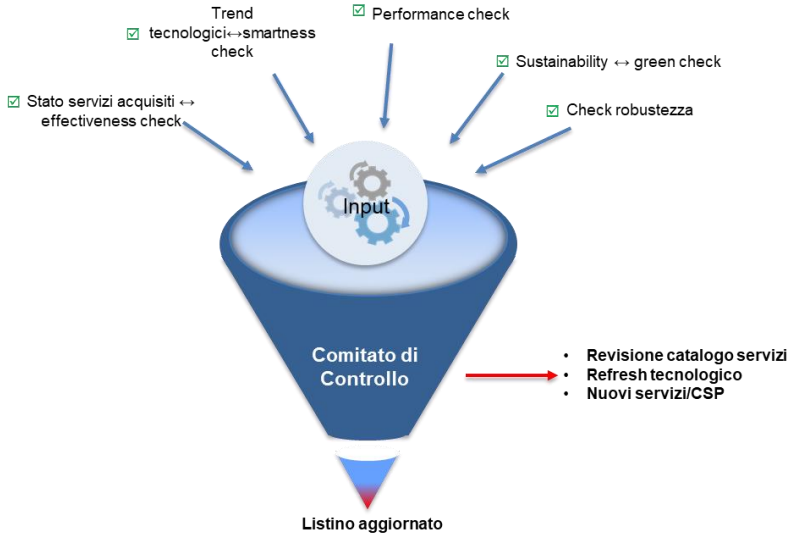



**Figura 21 Check identificativi**

- **evoluzione delle tecnologie** necessarie a rendere più "**smart**" la Pubblica Amministrazione, allo scopo di rispondere adeguatamente sia in termini tecnici che economici alle necessità del sistema Paese in accordo con le **linee guida del Piano Triennale della PA** e con i **trend di evoluzione tecnologica** proposti dal mercato;
- **verifica dello stato di obsolescenza** delle piattaforme tecnologiche presenti all'interno del PSN. Infatti, l'evoluzione continua dell'hardware e del software, nonché della offerta degli Hyperscaler, richiede un costante aggiornamento di tutta la piattaforma sia di gestione che di erogazione dei servizi per:
    - evitare un degrado delle prestazioni negli ambienti in uso – **performance check**;
    - ottenere un adeguato indice di sostenibilità, con particolare attenzione ai temi del green computing - **sustainability/green check –** come dettagliato nel capitolo relativo al criterio ID 15 (cfr. § **Errore. L'origine riferimento non è stata trovata.**);
    - garantire la resilienza e sicurezza della infrastruttura – **check di robustezza**.

I parametri oggetto delle verifiche (check) sopra descritte, sono, ove possibile, misurati tramite appositi indicatori, che potranno essere integrati e rivisti nell'arco della concessione: in particolare, vengono proposti i **KPI interni** riassunti in tabella:

*Tabella 6 KPI interni per misurazione dei parametri*

| Ambito | Descrizione | Metriche | Periodicità | Obiettivo |
|---|---|---|---|---|
| Amministrazioni Aderenti | % di Amministrazioni aderenti rispetto a quanto previsto nel periodo di riferimento | APSN= $\frac{Na}{NTOTx}$ %<br>Dove: Na= numero di amministrazioni aderenti<br>NTOT= num. di amministrazioni "candidate" a migrare | Semestre (rilevazione nei 30 mesi di finestra di adesione) | 100% |
| Utilizzo del servizio "x" | % di richieste per il "servizio x" a catalogo rispetto a quanto previsto nel PEF nel periodo di riferimento | UTILx= $\frac{Nx}{NTOTx}$ %<br>Dove: Nx= numero di richieste "servizio x"<br>NTOTx= num. di richieste previste nel periodo di riferimento | Anno | >95% |
| Indicatore di obsolescenza | % di server fisici (*) con età >= 3 anni | OBS= $\frac{So}{Stot}$ %<br>Dove: So= numero di server con età>=3 anni"<br>Stot= num. di server | Anno (rilevazione dal 36° mese in poi) | <=40% |
| Efficienza energetica dei server Industry Standard | % di CPU dei servizi Industry Standard (*) che rientrano nei primi venti posti del benchmark spec Power:<br>https://www.spec.org/ | CPUeff=$\frac{CPUok}{Cputot}$ %<br>Dove: CPUok= numero di CPU rientrante nei primi 20 posti del benchmark<br>CPUtot= num. Tot di cpu del servizio Industry Standard | Anno (rilevazione dal 36° mese in poi) | >= 30% |

(*) Esclusi i server in Housing

In aggiunta, verranno definiti specifici KPI derivati sia dai sistemi di monitoraggio degli asset infrastrutturali che dall'andamento del mercato IT. Tali KPI saranno associati a trigger e soglie specifiche che evidenzieranno al CdC la necessità di richiedere alla NewCo l'attivazione del processo di refresh tecnologico. A titolo di esempio, uno dei KPI potrebbe essere il superamento della soglia di consumi energetici previsti per quella determinata tipologia di server.

Verificata la necessità di un adeguamento tecnologico, la NewCo recepirà le indicazioni del CdC e provvederà ad avviare un iter competitivo tramite opportuni bandi di gara al fine di stabilire soluzioni best-in-class.

## 20.3 Modalità operative per la revisione dei prezzi

Sulla base dei check effettuati seguendo le linee d'azione per il controllo dei costi descritte al §20.2, vengono definite delle linee di intervento tecniche per la eventuale revisione dei prezzi, che possono prevedere:

- la revisione del Catalogo dei Servizi, con l'eventuale eliminazione di voci inutilizzate;
- il refresh tecnologico di parti della infrastruttura;
- l'inserimento di nuovi servizi.

Tali linee di intervento tecnico comportano in ogni caso dei cambiamenti alla infrastruttura di erogazione che devono essere congruiti con il PEF e quindi oggetto di analisi per valutare eventuali impatti sui prezzi. A tal fine il Concessionario adotta la modalità operativa schematizzata nella figura adiacente, che si caratterizza per la ciclicità delle tre fasi che la compongono e che descriviamo di seguito evidenziando, per ciascuna, obiettivi, attività e risultati attesi.

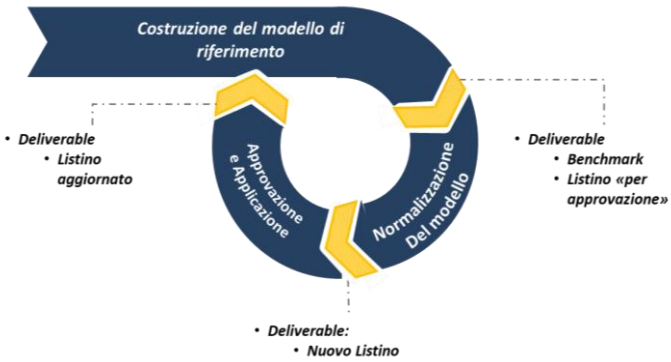



**Figura 22 Modalità operativa del Concessionario**

### Fase [1] Costruzione del modello di riferimento

Il CdC, svolgerà, direttamente o tramite terzi, un'approfondita indagine (benchmark) atta a rilevare i migliori prezzi di mercato per servizi analoghi a quelli erogati dal Concessionario e assegnati nell'ambito della Concessione.

Attraverso l'indagine di mercato saranno individuati i maggiori fornitori nazionali ed internazionali operanti sullo stesso perimetro di servizi oggetto della Convenzione: per ognuno di essi saranno raccolti i prezzi relativi.

I principali elementi alla base della valutazione saranno:

- equivalenza tecnica del servizio;
- equivalenza qualitativa (KPI) del servizio;
- durata del contratto;
- dimensione della fornitura.

I servizi oggetto di benchmarking sono tutti quelli riportati nel documento di gara Allegato 3 - sub 1-Progetto di Fattibilità proponente, oltre che eventuali nuovi servizi definiti durante il periodo della Convenzione, in aggiunta al listino iniziale.

Nel dettaglio è proposto il seguente modello:

- nell'ambito di ciascun servizio, viene confrontata ogni voce elementare (service element – corrispondente ad una riga di listino) con un set di analoghi elementi disponibili sul mercato (peer);
- per ciascun service element viene calcolato lo scostamento percentuale del valore di mercato medio rispetto a quello corrente di listino.

Per ogni servizio, oggetto di benchmark, saranno presentati al CdC, per la fase di valutazione:

- criteri di selezione e caratteristiche dei Gruppi di Riferimento, costituiti dall'insieme dei peer oggetto di analisi;
- i risultati di benchmark articolati in:
    - caratteristiche del servizio: codice, servizio, metrica, periodicità;
    - Market Place: numero riferimenti, media di mercato, differenza;
- la media di mercato è ottenuta dai prezzi dei peer selezionati per ogni servizio.

Nella presentazione dei risultati, effettuata servizio per servizio, verranno evidenziate con colori diversi le differenze percentuali rispetto ai riferimenti di mercato secondo la tabella seguente, che ha puro scopo illustrativo.

La scelta delle soglie è ispirata a prassi riscontrabili sul mercato dell'IT, in cui si rileva che in alcuni contratti di grandi dimensioni e di durata pluriennale è inclusa una clausola di benchmark obbligatorio

ogni 2-3 anni, con applicazione automatica dei risultati del benchmark nei casi in cui i valori di mercato si discostino dai prezzi praticati di almeno il 3-4%.

### Fase [2] Analisi e normalizzazione del modello, Confronto e sintesi della revisione

Sarà necessario condividere – Concedente e Concessionario – la metodologia che tenga conto degli elementi di analogia individuati in Fase [1]: i prezzi raccolti potranno essere normalizzati per renderli direttamente confrontabili con quelli in vigore nell'ambito della Concessione.

Il CdC, a seguito del consolidamento del benchmark e quindi della sua approvazione, predisporrà una "proposta di listino" che terrà conto dei risultati del benchmark stesso, congruente con quello sottoscritto con l'accettazione della Proposta di Concessione e che sarà sottoposta alla NewCo per accettazione e successiva implementazione.

Nel dettaglio tale "proposta di listino" sarà quindi composta tenendo conto dei seguenti criteri:

- valori di mercato rilevati tramite il benchmark;
- analisi delle effettive consistenze dei servizi acquisiti dall'insieme delle amministrazioni sottoscrittrici dei Contratti di Adesione;
- ipotesi di evoluzione del mercato e di utilizzo futuro dei servizi da parte delle amministrazioni;
- mantenimento della coerenza complessiva del listino prezzi e della sostenibilità del PEF.

| | |
|---|---|
| Valore compreso tra -4% e + 4% | |
| Valore minore di -4% | |
| Valore minore di -10% | |
| Valore maggiore di +4% | |
| Valore maggiore di +10% | |

*Tabella 7 Rappresentazione dei colori in base alle differenze percentuali*

A seguito della normalizzazione verrà prodotto il "nuovo listino" rappresentato nel file "adeguamentopricing.xls" originato dal file "Allegato 8 - Listino servizi" da sottoporre per approvazione al Comitato di Controllo.

### Fase [3] Approvazione e Applicazione

Il nuovo listino prezzi sarà oggetto di approvazione da parte del CdC, che ha la responsabilità di completare l'iter di verifica del benchmark e della proposta del nuovo listino alla NewCo.

I prezzi così ottenuti aggiornano il listino ed entrano in vigore con decorrenza il mese successivo a quello in cui si è conclusa la rilevazione dei prezzi. Non è prevista l'applicazione retroattiva del nuovo listino.

## 20.4 Cronoprogramma della Convenzione

Il processo di aggiornamento del listino prezzi, con le modalità operative precedentemente descritte, continua per l'intero arco della fornitura, a corredo della rivalutazione dei prezzi in funzione delle analisi periodiche sui trend di mercato e del rinnovo tecnologico.

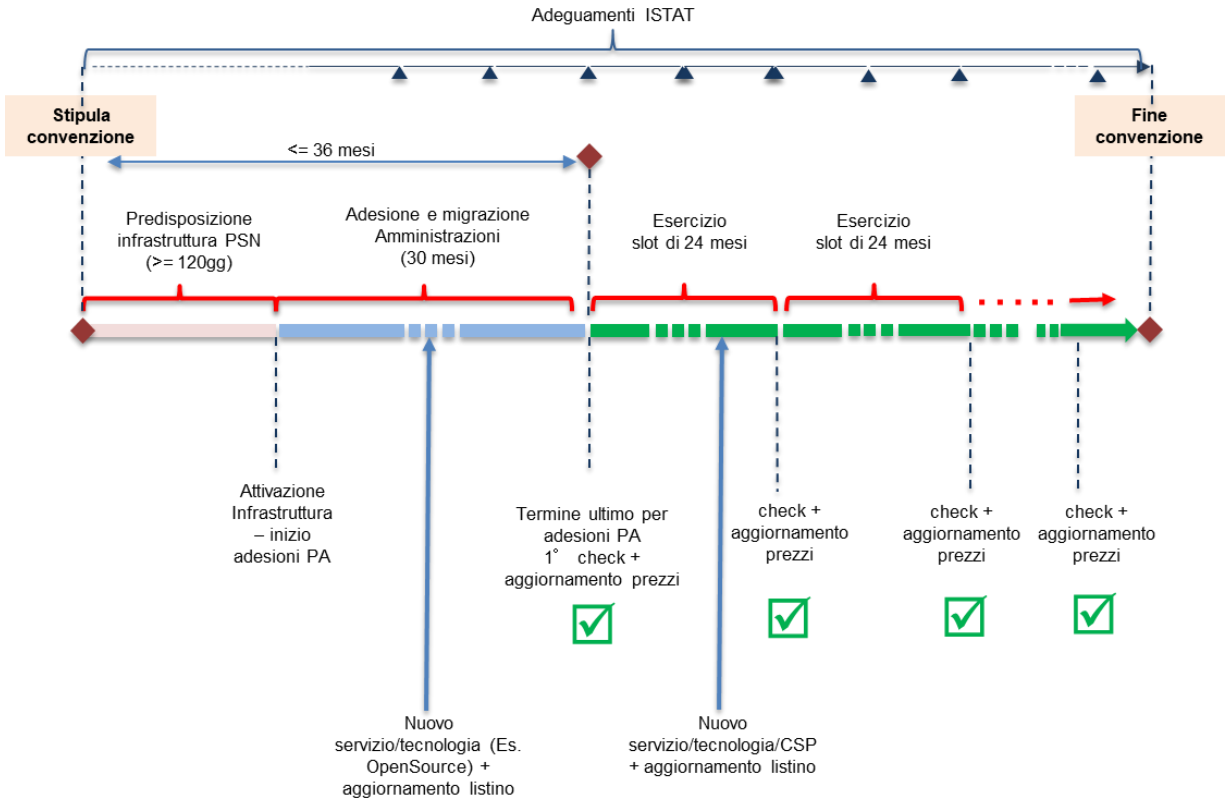



**Figura 23 Fasi di fornitura**

La figura sopra riportata (Figura 23) riassume il quadro sinottico delle fasi della fornitura con evidenza delle scadenze temporali degli aggiornamenti, evidenziati per ciascuna delle tre casistiche descritte (revisione (check) listino da parte del CdC – biennale; adeguamento ISTAT – annuale; introduzione di nuovi servizi - ad evento).

# 21 ID 19 – Valutativo - Miglioramenti sulla proposta progettuale per quanto riguarda gli aspetti relativi all'integrazione del PSN con l'Architettura Nazionale Cyber, con particolare riguardo alle modalità ed ai processi per l'integrazione con lo CSIRT Italia (fino a 1 punto), alla messa a disposizione di funzionalità per l'interazione con gli ISACs (fino a 1,5 punti), messa a disposizione di funzionalità di per scambio di informazioni A2A tra il SOC e lo CSIRT Italia (fino a 1,5 punti)

## 21.1 Executive Summary

Il Costituito RTI, in relazione alla premialità legata al miglioramento degli aspetti di cybersicurezza dell'infrastruttura, propone un'efficace integrazione del PSN con l'Architettura Nazionale Cyber, come di seguito descritto, nel completo soddisfacimento della richiesta espressa nel criterio ID 19.

La nuova organizzazione di **Cybersicurezza Nazionale** prevede un allineamento delle responsabilità relative alla sicurezza cibernetica in ambito nazionale/governativo a livello paese ad un livello omogeneo, e in qualche modo precursore, a quello europeo ed internazionale. Naturale evoluzione del processo avviato nel 2013 con il cosiddetto decreto Monti, proseguito nel 2017 con il successivo decreto Gentiloni e arricchito nel frattempo dalla pubblicazione di standard e linee guida strategiche (Quadro strategico nazionale per la sicurezza cibernetica), il Piano nazionale per la protezione cibernetica e la sicurezza informatica, oltre che naturalmente il **Framework Nazionale per la Cyber Security e la Data Protection** nei suoi vari rilasci, è la creazione **dell'Agenzia di Cybersicurezza Nazionale** e del **CSIRT Italia** quali soggetti principali autoritativi per la guida e l'indirizzo delle capacità di protezione e risposta in ambito di sicurezza cibernetica del paese. L'istituzione di perimetri nazionali ed europei di soggetti altamente sensibili anche in ambiente cibernetico, quali la direttiva NIS e il Perimetro di Sicurezza Nazionale Cibernetica, ha ovviamente aumentato gli obblighi di tali soggetti ma di conseguenza anche le attività di guida, vigilanza e controllo delle suddette istituzioni, realizzando un ecosistema di cybersicurezza nazionale capace di far fronte comune e reagire in maniera sistemica ma anche occasionale alle varie emergenze cibernetiche.

È quindi obbligo di fatto, per il PSN, **realizzare flussi informativi e strumenti che lo mettano in comunicazione con questo ecosistema nazionale** per poter aumentare significativamente le proprie capacità di rilevazione, protezione e risposta nell'ambito della cybersicurezza. Il **CERT** del PSN, realizzato

dal costituito RTI, oltre che proteggere il PSN dalle minacce cibernetiche, sarà anche responsabile di instaurare tutti quei flussi comunicativi proattivi e reattivi in grado di realizzare l'information sharing necessaria a essere parte integrante del sistema.

In particolare, sarà definita un'**Organizzazione di Sicurezza** all'interno della NewCo PSN e del costituito RTI con la nomina di soggetti responsabili in materia di cybersicurezza che agiranno da punti di contatto verso l'ACN e il CSIRT Italia. Questi potranno contare sulla collaborazione di tutte le strutture tecniche per l'assolvimento degli obblighi e l'implementazione dei requisiti cogenti in materia di cybersicurezza, comprese l'implementazione delle misure minime e dei controlli idonei al trattamento dei dati **Strategici, Critici e Ordinari**, la **notifica** e la gestione degli **incidenti** ed il mantenimento ed il miglioramento del livello di sicurezza nel corso della durata della Convenzione. Oltre all'ACN e al CSIRT Italia, saranno parte del "**Circle of Trust**" del PSN anche quegli **ISACs** (Information Sharing and Analysis Centers) nazionali ed europei che arricchiranno la base di conoscenza del PSN e allargheranno l'ecosistema di cybersicurezza con cui il PSN scambierà dati.

Allo scopo di massimizzare la rapidità e l'efficacia delle comunicazioni saranno utilizzati strumenti di scambio dati automatizzati (**A2A**) con il CSIRT e gli ISACs, quali piattaforme di **Cyber Threat Intelligence** (TIP) e Malware Information Sharing Platform (**MISP)**, largamente usate in questo ambito e quindi con utilizzo diffuso anche all'interno dei principali ISACs, allo scopo di ridurre al minimo i tempi di comunicazione, mantenendo altresì il controllo decisionale sui dati scambiati, il livello di affidabilità e i criteri di diffusione degli stessi.

## 21.2 Processi per l'integrazione con l'Architettura Nazionale di sicurezza e lo CSIRT Italia

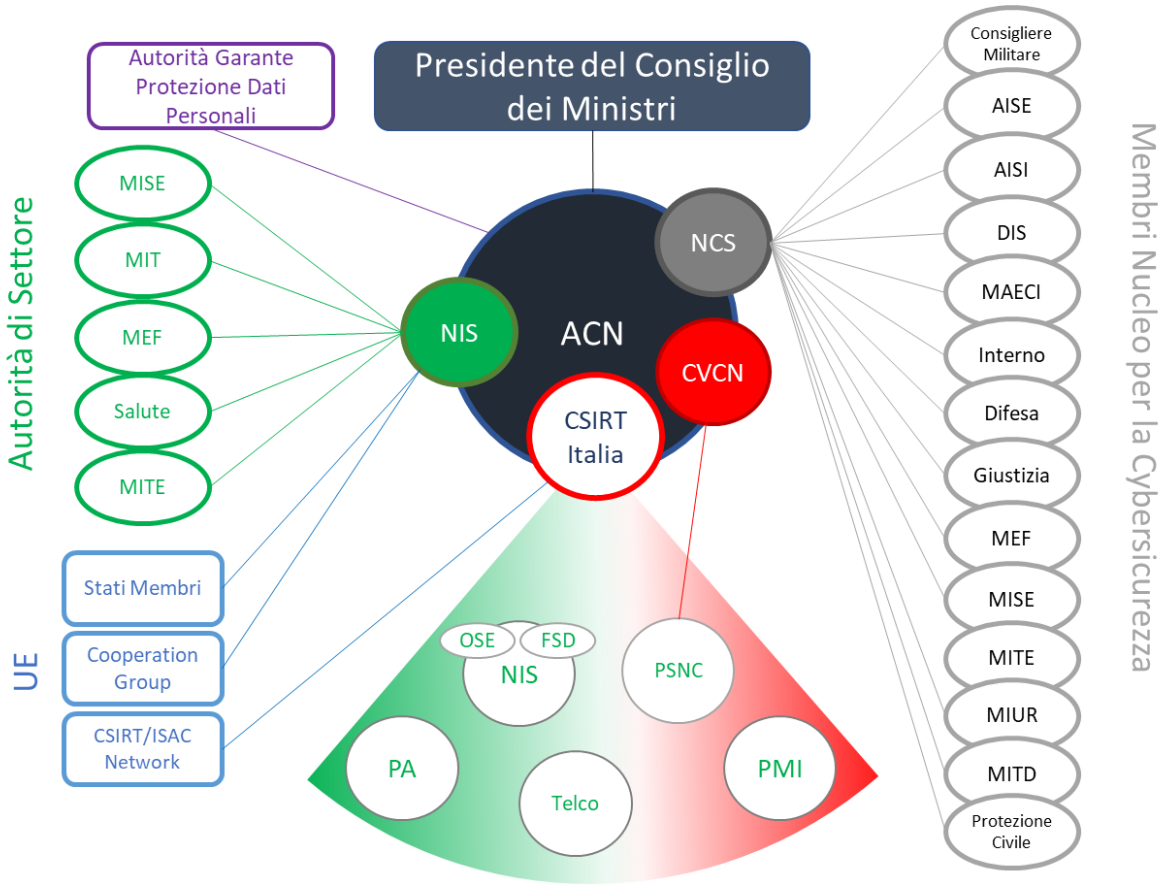



**Figura 24 Architettura Nazionale Cyber**

Il PSN, in qualità di Cloud Provider per il settore pubblico, rivestirà particolare importanza tra i fornitori di servizi digitali. La nuova Architettura Nazionale Cyber che vede la responsabilità del Agenzia per la Cybersicurezza Nazionale (di seguito ACN), oltre che sui vari standard di settore internazionali, è basata su importanti driver normativi che prevedono requisiti cogenti di cybersicurezza. Oltre al regolamento europeo GDPR (UE 2016/679) ed il D.Lgs. 196/2003 e ss.mm.ii che trattano la protezione dei dati personali, le normative di riferimento principali sono la **direttiva NIS** e la sua attuazione tramite D. Lgs. 65 del 2018, e il **Perimetro di Sicurezza Nazionale Cibernetica**, istituito tramite il D.L. 105 del 2019 (convertito con modificazioni dalla Legge 133 del 2019) ed esteso da altre leggi e decreti. Tra questi sicuramente riveste particolare importanza il Regolamento 628/2021 (e, nel rispetto degli atti esecutivi dello stesso Regolamento successivamente adottati dall'Agenzia per la cybersicurezza nazionale, d'intesa con il Dipartimento per la trasformazione digitale - le Determinazioni 306/2022 e 307/2022 e relativi allegati) che riporta al suo interno i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA, le caratteristiche di qualità, sicurezza,

performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione, estesi anche ai soggetti che ospitano le infrastrutture da cui vengono erogati i servizi delle PA (cfr. art.33-septies, comma 1, del **D.L. 179/2012 e ss.mm.ii.**). L'architettura di cybersicurezza nazionale vede all'interno dell'ACN diversi soggetti che svolgono già ruoli rilevanti per la cybersicurezza nazionale. L'ACN, infatti, rileva in toto le funzioni in questo ambito che erano già di AgID e MISE e si pone come autorità nazionale competente relativamente alla direttiva NIS con il compito di controllare l'effettiva conformità degli Operatori di Servizi Essenziali (OSE) e dei Fornitori di Servizi Digitali (FSD) alla direttiva. Al suo interno troviamo anche il CSIRT Italia, a cui competono principalmente: le attività di monitoraggio e gestione degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; la sensibilizzazione situazionale nonché la partecipazione alla rete dei CSIRT, ereditata dal DIS e il ruolo di **Centro di Valutazione e Certificazione Nazionale (CVCN)** ereditato dal MISE a cui è affidato il compito di effettuare la valutazione di beni, sistemi e servizi ICT destinati ad essere impiegati su infrastrutture che supportano la fornitura di servizi o di funzioni essenziali per lo Stato. Il PSN dovrà essere quindi inserito nell'ecosistema della cybersicurezza Nazionale e relazionarsi con i soggetti che la compongono nelle varie fasi delle sue attività. In particolare, in virtù anche e soprattutto del già citato Regolamento 628/2021 e successivi atti esecutivi ACN (di seguito "Regolamento 628/2021") il PSN dovrà interagire all'interno dell'architettura di cybersicurezza almeno con i seguenti soggetti:

- **CSIRT Italia** per le segnalazioni degli incidenti e tutte le attività relative alla gestione dei rischi e degli incidenti cyber;
- **ACN** per le relazioni riguardanti gli obblighi imposti dal Regolamento 628/2021 ed eventualmente gli altri perimetri normativi in cui il PSN potrebbe essere soggetto ad inserimento successivo;
- **CVCN** per il supporto alle verifiche imposte alle PA in perimetro PSNC;
- **Autorità garante per la protezione dei dati personali** per gli obblighi relativi al trattamento dei dati personali.

Il PSN dovrà essere progettato e implementato secondo i più avanzati standard di riferimento e consentire di poter realizzare quelle attività di assessment e controllo che la normativa prevede; in particolare:

**NIS** - D. Lgs. 18 giugno 2018, n. 65 attuativo della Direttiva (UE) 1148/2016 (c.d. Direttiva NIS)

- autovalutazione dello stato di esposizione al rischio cyber dei servizi essenziali erogati, in termini di mappatura dei livelli di maturità delle misure tecniche ed organizzative di sicurezza e di definizione degli interventi da implementare, la cui priorità è determinata sulla base dell'analisi del rischio;
- adozione delle citate misure tecnico/organizzative, sulla base del piano degli interventi definito;
- notifica senza giustificato ritardo al CSIRT Italia degli incidenti con impatto rilevante.

**PSNC** – Decreto-legge 105/2019 (convertito con modificazione dalla Legge 18 novembre 2019, n. 133):

- identificazione, in esito all'Analisi del Rischio, dei «Beni ICT», che in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo dell'integrità o della riservatezza dei dati/informazioni. Detti Beni ICT andranno comunicati all'ACN entro 6 mesi dalla ricezione della lettera di comunicazione di inclusione nel perimetro e aggiornati con cadenza annuale;
- notifica tempestiva degli incidenti con impatto sui Beni ICT o su servizi definiti «contigui»;
- adozione delle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, in conformità a quanto prescritto dal DPCM 81/2021;
- comunicazione al CVCN delle intenzioni di affidamento/acquisto di beni, sistemi e servizi ICT.

**Regolamento 628/2021**[2]

- implementazione misure di sicurezza e gestione delle attività di sicurezza;
- collaborazione con l'ACN in caso di crisi cibernetica;
- supporto alle attività di verifica e ispezione da parte del ACN;
- notifica e collaborazione in caso di incidenti cyber con il CSIRT Italia;
- notifica al ACN di richiesta di accesso, o accesso, da parte di soggetti extra-UE ai dati/metadati della PA;
- monitoraggio dei canali istituzionali del CSIRT Italia e ricezione di bollettini, aggiornamenti ed informazioni relative a minacce, attacchi e vulnerabilità di cybersicurezza;
- condivisione spontanea di informazioni in ottica infosharing con l'ecosistema nazionale e gli ISACs;

[2] Il Regolamento 628/2021 impatta direttamente anche il PSN, in virtù del art.33-septies, comma 1, del D.L. 179/2012 e ss.mm.ii

- disponibilità per l'ACN di report di vulnerabilità (OWASP, VA/PT) e altre informazioni relative ai controlli di sicurezza e infosharing.

Sono ovviamente validi anche gli obblighi in materia di protezione dei dati personali (GDPR - UE 2016/679 e D.Lgsl 196/2003 e ss.mm.ii.).

Il PSN dovrà permettere alle PA di garantire, sin dalla progettazione (by-design), il rispetto dei requisiti in materia di cybersicurezza, sopradescritti, per cui dovrà implementare contromisure e controlli di sicurezza idonei e consentire alle PA di essere conformi a tali obblighi, oltre che essere conforme ai controlli previsti dal Regolamento 628/2021 elencati agli allegati A, B, A2, B2 e C, in qualità di soggetto che detiene le infrastrutture digitali delle PA e di fornitore di servizi cloud. Tale conformità è abilitante per poter ospitare all'interno del PSN i dati delle PA catalogati in base ai criteri di classificazione in uso (ordinari, critici, strategici).

Pertanto, importanza rilevante sarà data alle relazioni con le autorità che sovraintendono le attività ed il controllo relativo alle principali normative impattate, che risiedono ora all'interno della Agenzia per la Cybersicurezza Nazionale, ed in particolare per la notifica degli incidenti al CSIRT Italia.

Il PSN nominerà, come previsto dalle normative, un **Incaricato** (e un suo sostituto) con il compito di gestire gli obblighi e le informazioni verso le istituzioni e un **Referente Tecnico** (e un suo sostituto) come referente verso il CSIRT Italia, per l'interlocuzione relativa alla gestione degli incidenti (la struttura completa dell'organizzazione è descritta più avanti e schematizzata in Figura 26). L'incaricato gestirà un'organizzazione interna al PSN (**Organizzazione di Sicurezza**) che si occuperà di gestire la sicurezza delle informazioni e degli asset del PSN e garantire la conformità ai requisiti cogenti. Gli estremi dell'Incaricato e del Referente Tecnico saranno comunicati all'ACN quali punti di contatto.

Tale Organizzazione di Sicurezza gestirà i contatti con tutte le entità che costituiscono l'ecosistema e l'architettura di Cybersicurezza Nazionale, con lo scopo di:

- ottemperare ai requisiti cogenti e garantire la conformità;
- instaurare e gestire un processo di collaborazione continuativa per migliorare il più possibile la gestione degli incidenti e delle crisi;
- supportare le istituzioni nei compiti di gestione della sicurezza e diffusione della consapevolezza e del senso di urgenza verso i clienti del PSN e ogni altro stakeholder.

Uno schema di processo, più generale, che comprende le interazioni anche con le altre strutture che compongono l'Architettura di Cybersicurezza Nazionale, e le piattaforme utilizzate a supporto dei processi è descritta nella figura 25. La figura mostra anche le interazioni con gli ISACs di settore ed il

CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche). Le piattaforme utilizzate per realizzare l'infosharing e gli automatismi A2A sono descritte nel paragrafo 21.3.

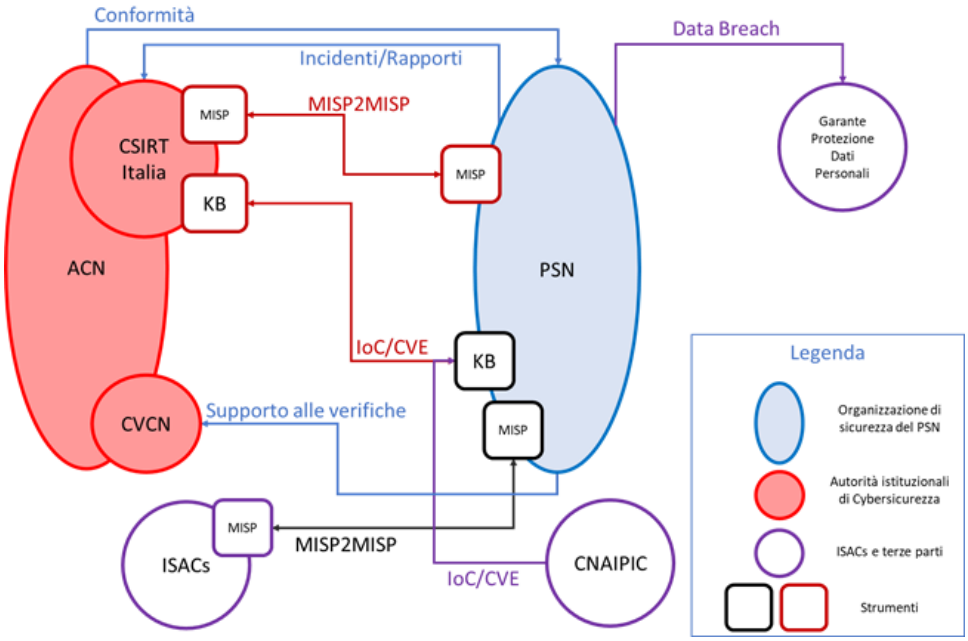



**Figura 25 Interazione tra PSN e autorità istituzionali nell'ambito della cybersicurezza**

In particolare, all'interno dell'Organizzazione di Sicurezza, saranno implementati almeno i flussi informativi, descritti nella tabella seguente.

Tabella 8 Processi di comunicazione con le istituzioni

| Processo | Attori coinvolti lato PSN | Attori coinvolti istituzionali | Tematiche | Frequenza |
|---|---|---|---|---|
| **Trasmissione o revisione delle modalità di adozione delle misure di sicurezza relative Regolamento 628/2021** | **Incaricato**, Referente Tecnico | ACN | Comunicazione al ACN delle modalità di implementazione delle misure tecnico/organizzative di sicurezza previste | Su richiesta |

| | | | | |
|---|---|---|---|---|
| **Notifica incidenti** | **Referente Tecnico**, Referente CERT | CSIRT Italia | Notifica al CSIRT Italia di un incidente di sicurezza con impatto rilevante. | In caso di incidente |
| **Notifica Personal Data Breach** | **DPO**, Referente Tecnico, Referente CERT, Referente IT | Autorità garante protezione dei dati personali | Notifica all'autorità garante di un avvenuto data breach con compromissione di dati personali | In caso di incidente |
| **Supporto alle verifiche Ispettive** | **Incaricato**, Referente Tecnico, altri su chiamata | ACN | Supporto alle attività ispettive di vigilanza svolte dal ACN per la verifica della effettiva attuazione di quanto prescritto dal Regolamento 628/2021 | Su richiesta |
| **Richiesta di autorizzazione accesso da parte di entità extra-UE** | **Incaricato**, Referente Tecnico | ACN | Il PSN segnala ogni richiesta di accesso a dati o metadati della PA proveniente da entità extra-UE e richiede autorizzazione all'accesso | Ad ogni richiesta |
| **Supporto alle verifiche su beni/servizi ICT** | **Incaricato,** Referente Tecnico, Referente IT | CVCN | Supporto del personale PSN alle verifiche di sicurezza sulle | Su ingaggio del CVCN |

| | | | | |
|---|---|---|---|---|
| | | | infrastrutture da parte del CVCN in caso di acquisto servizi PSN da una PA in perimetro PSNC | |
| **Trasmissione rapporti di vulnerabilità e/o Penetration Test e/o OWASP** | **Referente Tecnico** | CSIRT Italia | Trasmissione dei report di VA/PT eseguiti sui beni ICT in perimetro PSNC | Semestrale[3] |
| **Monitoraggio dei canali di comunicazione istituzionali del CSIRT Italia** | **Referente Tecnico**, Referente CERT | CSIRT Italia | Monitoraggio dei canali istituzionali di comunicazione e ricezione delle informazioni condivise | Ad ogni comunicazione |

Tali flussi potranno subire aggiornamenti sulla base delle modifiche alle normative o di specifiche linee guida emesse dall'ACN.

L'organizzazione, le modalità e i processi di integrazione con le autorità ed in particolare con il CSIRT Italia saranno inserite anche all'interno del **Piano di Sicurezza** (cfr. Progetto di Fattibilità del Proponente § 3). Il PSN adotterà processi e modalità di comunicazione con il CSIRT Italia abilitanti alla pronta gestione degli incidenti e al coordinamento operativo con lo stesso, anche mediante strumenti di condivisione delle informazioni specificati nel proseguo del paragrafo.

Il CSIRT Italia, come detto in precedenza, è il punto unico di contatto e organo responsabile del monitoraggio degli incidenti a livello nazionale, nonché dell'emissione di preallarmi, e altri tipi di informazioni divulgative in marito a rischi ed incidenti cyber.

[3] Come previsto nel Progetto di Fattibilità del proponente e dalle linee guida

I principali processi di comunicazione del PSN da e verso il CSIRT Italia da instaurare saranno per la comunicazione e la gestione degli incidenti e l'analisi del rischio, vista in particolare dal punto di vista della identificazione e valutazione delle vulnerabilità.

Per questi due processi, ma anche per gli obblighi normativi esposti precedentemente, il PSN intende strutturarsi con dei punti di contatto e una struttura interna, costituita dalla già introdotta **Organizzazione di Sicurezza**. Il punto di contatto primario con il CSIRT Italia sarà, all'interno del PSN, rappresentato dal **Referente Tecnico**, che sarà responsabile di notificare gli incidenti, comunicare i rapporti di vulnerabilità e di Penetration Test eseguiti sulle infrastrutture, oltre a qualsiasi altra attività di supporto e di gestione incidenti/crisi.

Il Referente Tecnico, collabora in stretta sinergia con l'Incaricato, e potrà contare nell'espletamento dei suoi compiti sulla collaborazione delle strutture di cybersicurezza del PSN (Referenti SOC e CERT), oltre a quelli designati delle altre funzioni tecniche (Referenti IT).

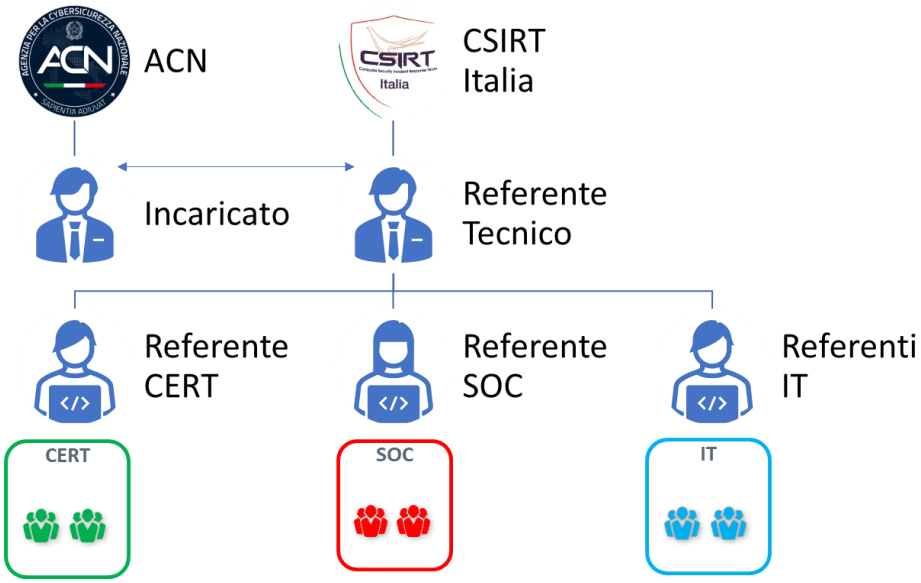



**Figura 26 Organizzazione ufficio di sicurezza PSN e processi CSIRT**

Di seguito sono descritte modalità e processi principali previsti **per l'integrazione con il CSIRT Italia**:

- **notifica di incidente**: il processo si sviluppa nelle seguenti fasi:
    1. rilevazione: il Referente Tecnico riceve la segnalazione di incidente dal CERT del PSN;
    2. valutazione: il Referente Tecnico in collaborazione con l'organizzazione di sicurezza verifica gli impatti sulle Amministrazioni, nonché l'impatto complessivo sul PSN;

3. attestazione: il Referente Tecnico procede alla ufficializzazione della sussistenza dell'incidente;
4. registrazione/classificazione dell'evento: Il Referente Tecnico provvede alla registrazione della segnalazione ed alla classificazione dell'evento; da tale momento sono misurate le tempistiche previste per l'invio della comunicazione;
5. notifica e redazione report: il Referente Tecnico, in collaborazione con l'Organizzazione di Sicurezza predispone la documentazione contenente le informazioni richieste dagli obblighi normativi procede alla notifica alle Amministrazioni impattate secondo le tempistiche previste dal Regolamento 628/2021 e cioè entro 1 ora per eventi con impatti rilevanti, e successivamente con segnalazione spontanea anche al CSIRT Italia;
6. archiviazione: l'Organizzazione di Sicurezza procede all'aggiornamento dell'inventario con la lista di tutti gli incidenti e supporta le comunicazioni con l'Amministrazione ed il CSIRT Italia nelle successive fasi di gestione e rientro;
7. modalità: l'incidente viene notificato utilizzando le funzionalità del portale del CSIRT Italia, e le credenziali di accesso fornite al Referente Tecnico (o suo sostituto), anche con l'utilizzo di strumenti semiautomatici (workflow autoritativi) descritti nel proseguo del documento.

- **notifica di rapporto Penetration Test (PT): il Referente Tecnico**, si assicura dell'esecuzione delle attività di PT, sulla base delle scadenze definite nel Progetto di Fattibilità del Proponente. Con riferimento a tali tempistiche, è inviato con cadenza semestrale[4], o quando disponibile, il rapporto di esecuzione del Penetration Test più recente;
- **modalità**: il rapporto viene trasmesso via e-mail utilizzando la chiave PGP del CSIRT, identificando nell'e-mail l'ID univoco del soggetto;
- **notifica di rapporto di Vulnerability Assessment** (VA): il Referente Tecnico, si assicura dell'esecuzione delle attività di VA e invia quando disponibile, il rapporto di esecuzione del Vulnerability Assessment più recente;
- **modalità**: il rapporto viene trasmesso via e-mail utilizzando la chiave PGP del CSIRT, identificando nell'e-mail l'ID univoco del soggetto;
- **monitoraggio dei canali di comunicazione istituzionali del CSIRT Italia**: Il Referente Tecnico, in collaborazione con il referente CERT e il CERT del PSN monitorano, anche con l'utilizzo degli

[4] Come previsto nel Progetto di Fattibilità del proponente e dalle linee guida

strumenti A2A descritti nel proseguo del paragrafo, i canali istituzionali di comunicazione del CSIRT, quali portale e e-mail, e recepiscono gli avvisi e le pubblicazioni;

- **modalità:** Utilizzo del Portale del CSIRT Italia e monitoraggio delle caselle e-mail di contatto comunicate al CSIRT stesso.

## 21.3 Funzionalità A2A per scambio di informazioni con il CSIRT Italia

Per realizzare le attività di info sharing, minimizzando i tempi di risposta agli incidenti e massimizzando la condivisione di informazioni relativamente a malware, incidenti, minacce e agenti di minaccia, oltre che per supportare le capacità di detection e reaction interne, il PSN avrà a disposizione, la propria Knowledge Base; la **Knowledge Base (KB) di sicurezza** del PSN sarà costruita sull'esperienza e le informazioni dei membri del costituito RTI, ed in particolare di Leonardo, tramite utilizzo di piattaforme di security intelligence quali SIEM, CTI, accesso a feed interni e professionali relativi a malware, IoC e vulnerabilità, e lo scambio informativo con organizzazioni paritetiche (ISACs), il CSIRT Italia e le altre autorità competenti. Sarà disponibile fin dal go live del PSN, mutuando ed utilizzando la grande quantità di informazioni già collezionate grazie all'esperienza acquisita nei confronti di clienti, in particolare nel settore della PA, e sarà continuamente arricchita dai dati raccolti internamente ed esternamente al PSN.

La knowledge base è inoltre supportata dall'utilizzo della soluzione proprietaria **Threat Intelligence Platform (TIP)** di Leonardo. I workload di raccolta, analisi e diffusione delle informazioni di Cyber Threat Intelligence sono eseguiti su un'infrastruttura **High Performance Computing** dedicata esclusivamente a questo scopo, in grado di trattare grandi quantità di dati. La piattaforma permette l'acquisizione di numerose tipologie di informazioni relative alla Cyber Security, quali **IoC**, **vulnerabilità**, informazioni su **minacce** e **agenti** di minaccia, **tecniche di attacco** (TTP), e mette a disposizione degli analisti di intelligence diversi strumenti per massimizzare l'efficacia delle attività di analisi, arricchimento, categorizzazione, validazione e diffusione delle informazioni di intelligence. La piattaforma dispone di interfacce applicative (Machine to Machine) e tool di visualizzazione avanzata per la ricerca ed il tagging delle informazioni raccolte e la definizione di eventi ed entità basati su una **Ontologia** e una **Tassonomia Cyber proprietaria**, basata sul **Diamond Model** (capace di descrivere le 4 principali caratteristiche di un incidente/evento avverso - cfr. Figura 27), e definita sulla base di framework più diffusi (MITRE ed ENISA su tutti) e pienamente compatibile con questi. In aggiunta la piattaforma supporta l'analisi avanzata e la validazione anche con strumenti ed algoritmi/modelli di **deep/machine learning**, introducendo e sfruttando i concetti di **AI** all'interno del servizio, riuscendo a correlare una grande quantità di informazioni e sfruttando i "segnali deboli" che solo motori di AI possono individuare. Il tutto ha permesso nel corso del tempo al personale del RTI costituito di realizzare una **Knowledge Base** di Cyber

Threat Intelligence di ampio respiro, ma con forti specializzazioni **sull'Italia** ed in particolare sul comparto della **Pubblica Amministrazione**.

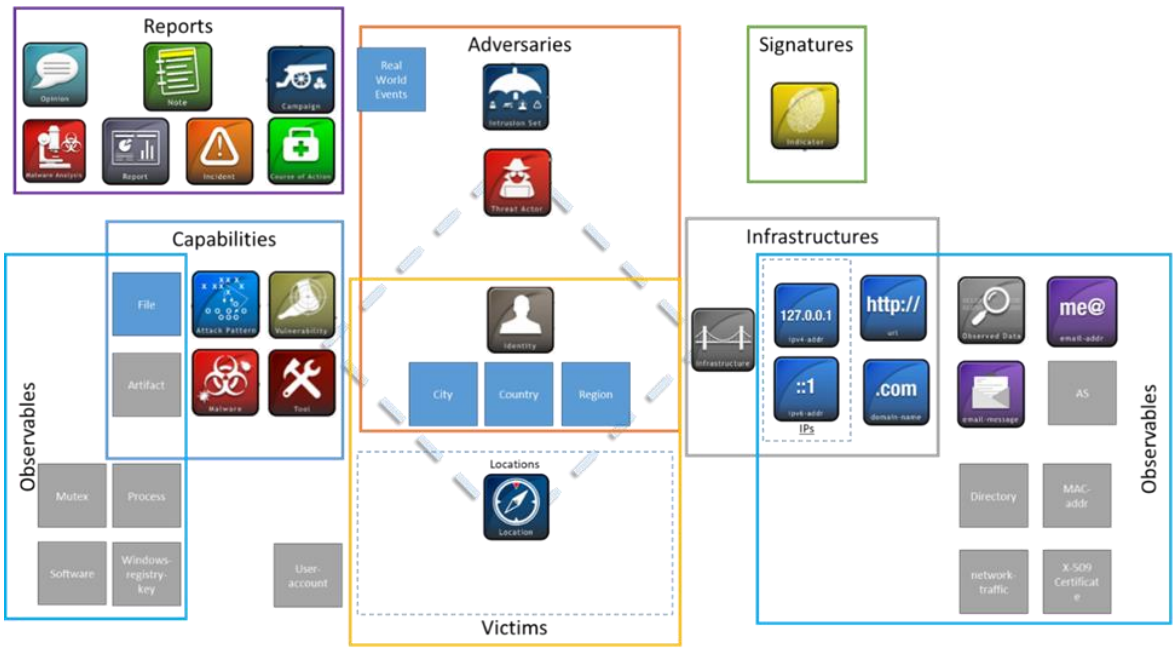



**Figura 27 Diamond Model**

Lo scambio dati tra il PSN, ed in particolare il CERT del PSN, e CSIRT Italia riveste particolare importanza data la natura dei servizi erogati che caratterizzano di fatto il PSN come Fornitore di servizi digitali di primaria importanza in ambito italiano e che riveste dunque un ruolo rilevante in ambito Nazionale.

Vista la natura rapida e immediata della diffusione di attacchi e incidenti nel cyberspazio tale scambio di dati deve essere supportato da protocolli di automazione per lo scambio di informazioni, per permettere la tempestiva e puntuale risposta a qualsiasi tipo di minaccia o incidente.

Proprio per velocizzare e migliorare la comunicazione, il CERT del PSN implementerà delle funzionalità A2A (Application to Application) dedicate al CSIRT per la ricezione in automatico delle segnalazioni relative a incidenti, minacce, IoC, eventi di interesse che il CSIRT intende segnalare al PSN, e viceversa dati in uscita dal PSN verso il CSIRT Italia, attraverso l'accesso alle informazioni memorizzate all'interno della KB di sicurezza del PSN, che saranno quindi rese disponibili al CSIRT Italia. Per tali automazioni saranno utilizzati i seguenti strumenti:

- **Knowledge Base di Sicurezza**, ossia la piattaforma **TIP** precedentemente citata, che detiene le informazioni e ne permette l'analisi;
- **Security Orchestration, Automation and Response** (**SOAR**) del PSN, che permette l'integrazione con le piattaforme di sicurezza del PSN (SIEM, Threat Intelligence, sonde e sensori, endpoint &

data protection) e l'automazione tramite playbook di workflow che permettono l'arricchimento, l'analisi e l'enforcement automatico dei dati ricevuti e/o da inviare;

- **Malware Information Sharing Platform** (**MISP**) per la condivisione di informazioni relative alla cybersicurezza (per la descrizione della piattaforma MISP vedi di seguito Funzionalità per l'interazione con gli ISACs).

In particolare, saranno implementati i seguenti flussi informativi A2A:

- **importazione di dati dal CSIRT**: saranno implementate policy di filtro sugli IoC comunicati, tramite playbook automatici della piattaforma SOAR del PSN, mediante l'aggiornamento di liste di Hash, IP, URL e domini malevoli. Gli IoC prodotti e pubblicati dal CSIRT Italia saranno importati automaticamente, in ottica di actionable intelligence, all'interno delle piattaforme del PSN, e implementeranno blocchi e filtri sull'intera infrastruttura. I dati potranno essere importati nei formati CSV, STIX, XML, JSON e OpenIOC. I playbook tramite un processo semi-automatico con autorizzazione manuale implementeranno direttamente sull'infrastruttura di sicurezza del PSN gli IoC ricevuti. Tale processo così implementato consentirà la ricezione puntuale delle segnalazioni da parte del CSIRT Italia, e il processo autorizzativo consentirà al CERT del PSN di analizzare le informazioni ricevute, implementare tutti i processi di valutazione degli impatti e dell'urgenza, per poi automatizzare l'implementazione (enforcement) direttamente tramite piattaforma SOAR. L'import di tali informazioni sarà realizzato utilizzando le seguenti interfacce A2A:
  - **HTTP/HTTPS** IoC – monitoraggio continuo dei server HTTP (o altri protocolli) utilizzati per la pubblicazione di feed da parte del CSIRT Italia;
  - **STIX/TAXII** – utilizzando il protocollo di trasporto TAXII (Trusted Automated eXchange of Indicator Information), con i dati tipicamente in formato STIX;
  - **MISP2MISP** – utilizzano i protocolli disponibili all'interno delle piattaforme MISP;
- esportazione di dati verso il CSIRT: il CSIRT potrà avere accesso alla KB di sicurezza del PSN, implementata tramite la piattaforma TIP precedentemente descritta, allo scopo di fornire supporto in caso di incidenti o ottenere informazioni relativamente a IoC o minacce rilevate dal CERT del PSN. L'accesso ai dati permetterà al CSIRT Italia di ottenere in modalità istantanea e tempestiva le informazioni di sicurezza dal PSN, tra cui, incidenti, eventi, minacce, TTP (Techniques, Tactics, Procedures), agenti di minaccia, IoC, informazioni sui target degli attacchi ed altro. L'accesso alla piattaforma potrà avvenire tramite le seguenti modalità:

- **REST API**, con cui il PSN fornirà una serie di Query per l'interrogazione della Knowledge base;
- **STIX/TAXII** per l'esportazione dei dati in formato STIX (Structured Threat Information eXpression), relativamente alle minacce informatiche;
- **MISP2MISP**, con l'accesso ad una piattaforma MISP dedicata.

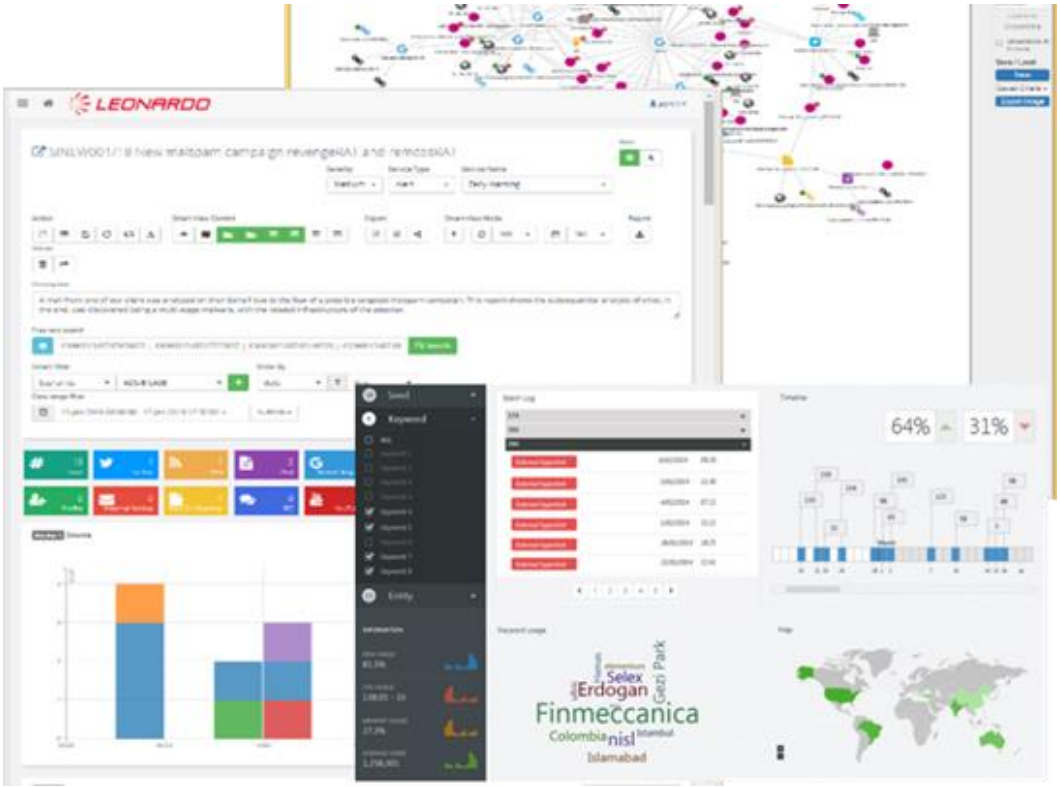



**Figura 28 Knowledge Base di Sicurezza e piattaforma TIP**

Le informazioni scambiate tramite strumenti A2A utilizzeranno il protocollo TLP (Traffic Light Protocol) per l'implementazione dei principi di **need-to-know** e **need-to-share**, descritto nel successivo paragrafo (cfr. Figura 31).

Le modalità di accesso alla piattaforma saranno concordate con il CSIRT stesso, privilegiando connessioni di tipo P2P (Point to Point), con accesso controllato tramite credenziali scambiate con canali alternativi.




**Figura 29 Form di comunicazione incidenti al CSIRT Italia**

Inoltre, saranno automatizzate, in ottica A2A, tramite playbook, le segnalazioni di incidente verso il CSIRT Italia. Al verificarsi di incidenti di particolare rilevanza, tramite un workflow semi-automatico implementato sulla piattaforma SOAR del CERT, con iter approvativo manuale, gli incidenti saranno notificati tramite il popolamento automatico dei parametri del form o tramite le API messe a disposizione dal CSIRT Italia stesso. Questo consentirà di estrarre in maniera automatica dalla KB di sicurezza del PSN tutti i dati utili a popolare i campi richiesti per le segnalazioni, a predisporre il completamento manuale dei dati mancanti, e inviare tempestivamente le stesse.

## 21.4 Funzionalità per l'interazione con gli ISACs

La cooperazione con gli ISACs (Information Sharing & Analysis Center) sarà uno degli aspetti fondamentali inclusi tra le attività del PSN per raggiungere quel livello di condivisione delle informazioni a livello nazionale ed europeo necessario per garantire la migliore capacità di prevenzione e risposta agli incidenti. La partecipazione alla rete di interscambio di informazioni con gli ISACs permetterà di:

- condividere informazioni relative ad incidenti e alla cybersecurity in generale;
- avere accesso in caso di necessità a competenze e conoscenze esterne;
- acquisire conoscenza riguardo il livello di sicurezza nei settori critici;
- possibilità di cooperazione gestita centralmente in caso di pandemie;
- condividere la conoscenza e l'esperienza sui principali attori e sulle più rilevanti minacce cyber.

Il PSN costruirà perciò il proprio "Circle of Trust" con gli ISACs che concorreranno alla costruzione della propria Knowledge Base di sicurezza. Saranno privilegiati i rapporti con ISACs aventi focus sul territorio nazionale ed europeo e sul settore della Pubblica Amministrazione.

La condivisione di informazioni verterà principalmente sullo scambio di dati relativi a minacce, vulnerabilità, tecniche di attacco o mitigazione, leading practice nel mondo cyber e analisi strategiche.

I rapporti con gli ISACs che già sono o saranno parte del "Circle of Trust" saranno gestiti principalmente con strumenti tecnici di tipo "information sharing", che condivideranno le informazioni da e verso la Knowledge Base di sicurezza del PSN.

Le informazioni e gli eventi di interesse saranno scambiati tramite una piattaforma tecnologica di tipo **MISP** (Malware Information Sharing Platform) dedicata agli ISACs, che permette la condivisione di informazioni basata sui concetti di evento e entità. MISP permette lo scambio di informazioni verso altri sistemi MISP e/o verso altre piattaforme di Cyber Threat Intelligence tramite l'utilizzo dei più diffusi protocolli di trasporto di information sharing e una tassonomia comune e universalmente utilizzata. MISP è lo strumento ad oggi più diffuso a livello internazionale per la condivisione di informazioni relative alla Cyber Threat Intelligence ed è utilizzato da tutti i principali ISACs, CERT governativi e di settore europei e mondiali e i principali CERT delle più importanti aziende industriali mondiali.

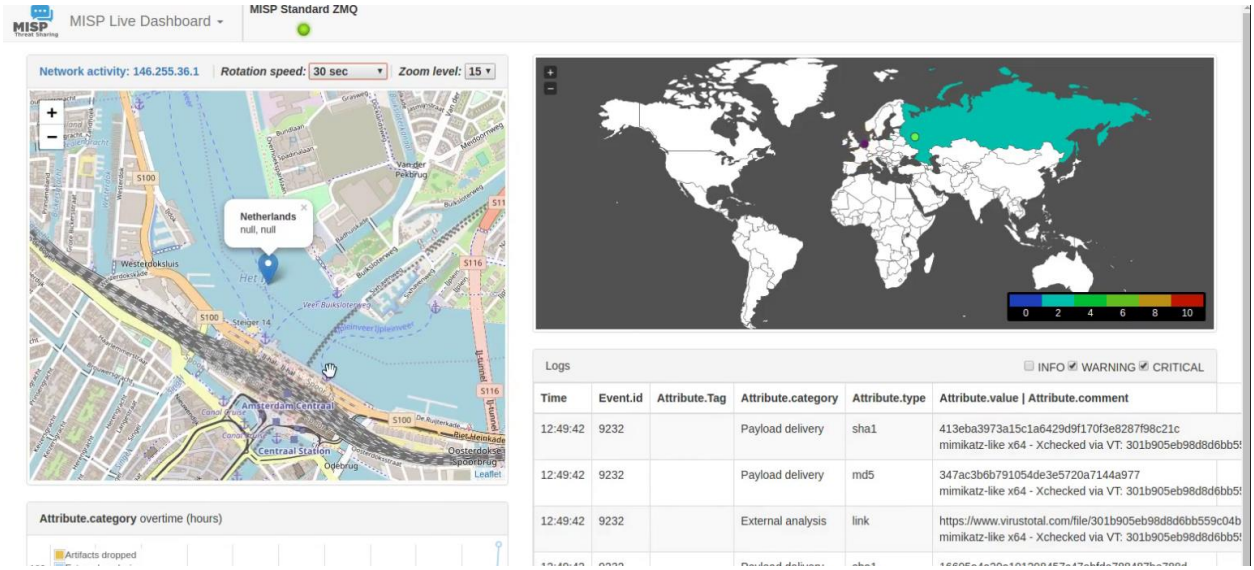



**Figura 30 MISP Dashboard**

La sincronizzazione tra le istanze MISP potrà avvenire, in base agli accordi, nelle due modalità **push**, in cui il MISP del PSN invierà gli eventi selezionati e le informazioni alle altre istanze MISP degli ISACs, o **pull**, in cui il MISP del PSN risponderà alle interrogazioni per la sincronizzazione.

Le informazioni scambiate tramite MISP utilizzeranno il protocollo TLP (Traffic Light Protocol) per l'implementazione dei principi di **need-to-know** e **need-to-share**, e restringere e controllare la diffusione delle informazioni solo per gli aventi diritto.

| | TLP: RED<br>Diffusione vietata<br>Solo destinatari | TLP: AMBER<br>Diffusione limitata<br>Organizzazioni destinatarie | TLP: GREEN<br>Diffusione limitata<br>Solo all'interno della comunità | TLP: WHITE<br>Diffusione illimitata |
|---|---|---|---|---|
| Limitazioni | | | | |
| Quando utilizzarlo | Impatto su privacy, reputazione o operatività | Rischio su privacy, reputazione o operatività se diffuso all'esterno | Informazioni utili per le organizzazioni affiliate e comunità più ampie | Nessun rischio legato alla diffusione. Adatto alla diffusione pubblica |
| Come utilizzarlo | Solo destinatari | Solo membri delle organizzazioni | Membri della comunità e partner Non adatto alla diffusione pubblica | Nessuna restrizione |

**Figura 31 TLP e restrizioni**

Tale protocollo (TLP) sarà utilizzato anche per lo scambio di informazioni basato su altri mezzi. Oltre agli strumenti automatici, infatti, è uso comune tra gli ISACs utilizzare anche altri metodi di scambio informativo che prevedono anche:

- meetings e incontri per scambio reciproco;
- working groups su tematiche di interesse;
- partecipazioni a conferenze ed eventi;
- e-mail, newsletters e teleconferences.

In particolare, per garantire la riservatezza dei dati scambiati con questi strumenti, oltre al protocollo TLP sono usati strumenti di cifratura basati sul principio del Web/Circle of Trust (es. PGP/GPG).

# 22 ID 20 – Valutativo - Completezza, accuratezza e verificabilità del metodo che il concorrente si impegna ad adottare per la definizione del dimensionamento delle risorse (giorni/uomo e relativo team mix per tipologia di strategia di migrazione) e delle tempistiche per la realizzazione di ciascuna fase di ciascun progetto di migrazione per gli scenari 1, 2 e 3 e per i casi di "breve termine" e "medio e lungo termine"

## 22.1 Executive Summary

L'esecuzione della migrazione in cloud all'interno dell'infrastruttura del PSN da parte di una amministrazione aderente è una progettualità che richiede **un'accurata fase di pianificazione in termini di risorse e tempistiche**, al fine di garantire il raggiungimento degli obiettivi prefissati, in relazione alla premialità del miglioramento richiesta dal criterio ID 20.

Il costituito RTI applicherà tutte le *best practice* sviluppate nel tempo nell'ambito di numerosi progetti di onboarding e trasformazione cloud erogati verso servizi ed infrastrutture di molte Amministrazioni, grazie alle esperienze Leonardo, Sogei e Tim in questo specifico ambito.

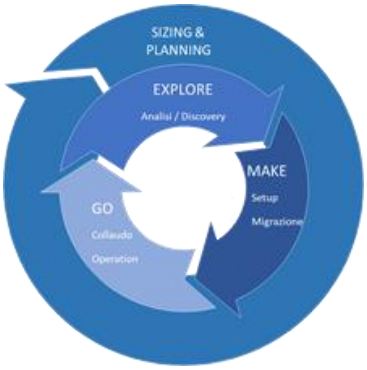



**Figura 32 Framework EMG2C**

Viene adottato un **framework metodologico** proprietario **EMG2C** (**Explore, Make, Go to Cloud**), rappresentato in Figura 32 e descritto nel dettaglio nel par. 22.6, che permette di utilizzare approcci alla migrazione sia di tipo **Waterfall (scenari di tipo legacy)** sia di tipo **Agile SCRUM**, che aiuta a creare valore attraverso un percorso di adattamento alle attività complesse. Il framework proposto dal costituito RTI si completa con **un approccio metodologico di Sizing & Planning dei progetti** finalizzato al **dimensionamento delle risorse e le tempistiche di ciascuna fase della migrazione**, e che garantisce **completezza, accuratezza e verificabilità**, integrando **i 2 criteri di dimensionamento previsti all'interno del Progetto di Fattibilità** (Dimensione dell'Amministrazione e Livello di Cloud Maturity dell'Amministrazione), **con ulteriori 4 variabili dimensionali**, la cui valorizzazione sarà garantita dagli input raccolti nella fase di Analisi/Discovery (es. complessità dei dati gestiti in base alla classificazione sulla base dei criteri dell'Agenzia per la Cybersicurezza, complessità dei servizi oggetto di migrazione, conoscenza del contesto dell'Amministrazione, disponibilità e maturità della documentazione di riferimento presso l'Amministrazione).

Tali integrazioni permettono di definire **un modello di stima che copre tutte le fasi di progetto e per tutti i possibili scenari progettuali** (alta, media e bassa complessità) e relativi orizzonti temporali (breve termine e medio/lungo termine). A scopo illustrativo ed esemplificativo dell'applicazione del modello proposto, all'interno del documento sono presentati **3 Use Case progettuali** che simulano possibili scenari di migrazione a complessità differente *(Best Case, Worst Case, Mixed Case)* attraverso **le diverse valorizzazioni delle variabili dimensionali** previste per ciascun progetto.

Per l'ID20, nel documento sarà fornita prima la proposta metodologica per la **definizione del dimensionamento delle risorse e delle tempistiche** (cfr. paragrafo 22.2), successivamente **una descrizione dell'approccio metodologico proposto** dal costituito RTI **per l'esecuzione di ciascuna delle fasi di progetto individuate nel Progetto di Fattibilità** (Analisi/Discovery, Setup, Migrazione, Collaudo) (cfr. paragrafo 22.3 e 22.4) e, infine, **3 Use Case operativi di applicazione del modello descritto** (cfr. paragrafo 22.5) [5], e successivamente **una descrizione dell'approccio metodologico proposto** dal costituito RTI **per l'esecuzione di ciascuna delle fasi di progetto individuate nel Progetto di Fattibilità** (Analisi/Discovery, Setup, Migrazione, Collaudo) (cfr. paragrafo 22.6).

In merito alle attività di medio e lungo termine legate al cloud enabling dell'Amministrazione, il costituito RTI applicherà il medesimo modello di seguito rappresentato. Chiaramente, l'obiettivo delle fasi di Analisi/Discovery sarà in questo caso finalizzata agli interventi di re-platform o re-architect decisi dall'Amministrazione e quindi necessiterà di un delta di analisi rispetto a quella prevista per il breve termine. Questa attività sarà svolta con il medesimo team Mix di migrazione, più eventuali figure definite nell'ambito del MIX dei Professional Service che dovessero risultare necessarie e che definiranno il progetto di trasformazione, i modi e i tempi secondo il modello rappresentato.

## 22.2 Approccio metodologico al dimensionamento risorse e tempistiche del Piano di Migrazione

Ai fini di un corretto dimensionamento in termini di effort (giorni/uomo), team mix e tempistiche previste per ciascun Piano di Migrazione, il costituito RTI prevede di adottare una metodologia per **la pianificazione ed il dimensionamento**, già sperimentata in numerosi progetti già condotti dalle singole

[5] In merito agli use case per medio e lungo termine si è pensato che le differenze specifiche e puntuali di ciascuna amministrazione rispetto ad un criterio medio, facilmente applicabile per operazioni di Lift&Shift, ma molto più articolato e complesso per operazioni di cloud enabling di re-platform o re-architect, risultasse poco attendibile e si è preferito non esporre casi d'uso in questo ambito. Chiaramente la metodologia resta esattamente la stessa e la condivisione di dettaglio che verrà fornita per i singoli interventi richiesti, fornirà, grazie ai criteri metodologici descritti, una verificabilità oggettiva all'Amministrazione per questa tipologia di trasformazioni.

Società, modulabile secondo la complessità dello specifico progetto (scenario 1,2,3) ed in base alla strategia di migrazione individuata (breve termine o medio/lungo termine).

Il metodo, come meglio dettagliato più avanti, si articola sulle varie fasi del progetto di migrazione (Analisi/Discovery, Setup, Migrazione, Collaudo).

Utilizzando la metodologia Agile e le sue tecniche, Il **processo di pianificazione** prevederà sin dall'inizio il numero e la tipologia di risorse necessarie a gestire tutte le diverse fasi della Migrazione, ma sarà più preciso nel breve termine e andrà confermato durante l'avanzamento delle attività. La programmazione a lungo termine permetterà di valutare le eventuali sovrapposizioni di obiettivi e il processo di pianificazione continua aiuterà ad evitare l'aumento improvviso dei carichi di lavoro.

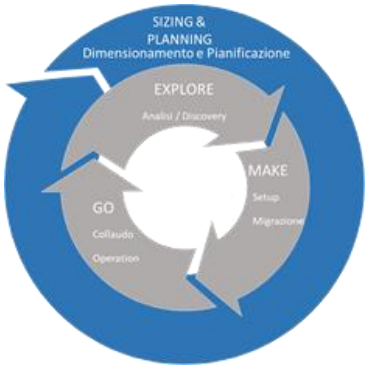



**Figura 33 Fasi del progetto di migrazione**

Il processo è basato sulle seguenti macro-fasi:

- **pianificazione attività:** pianificazione per ciascuna fase (Analisi/Discovery, Setup, Migrazione e Collaudo) delle attività con il massimo livello di dettaglio per le attività più prossime, tenendo sotto controllo in modo centralizzato tutti i possibili eventi che possano causare sovrapposizioni e picchi di attività. Utilizzando il concetto di miglioramento continuo, è possibile rivedere la pianificazione in diversi momenti, rivalutando le specifiche iniziali dei singoli stati e le variazioni che sono emerse durante le varie fasi di lavorazione. In questo modo è possibile fare un'analisi accurata dei trend di lavoro, della programmazione dei progetti e del rispettivo stato di avanzamento;
- **identificazione e quantificazione dell'effort**: valutazione delle figure professionali da impiegare, sulla base delle esigenze rilevate e delle attività da svolgere, secondo i criteri quanto più oggettivi descritti in seguito, al fine di identificare le competenze più adatte e abilitare la costituzione di Team per le singole fasi che rispondano alle effettive necessità, consentendo all'Amministrazione un pieno controllo e consapevolezza su dimensionamento e tempistiche del progetto;
- **definizione team operativi:** allocazione e la schedulazione puntuale del Team di Progetto e l'ipotesi di distribuzione delle risorse che saranno impiegate nello svolgimento delle attività.

Il **processo di dimensionamento** si sviluppa in fasi che prevedono **la stima del bacino di disponibilità delle risorse** da cui verranno selezionate quelle che comporranno i Team di Progetto, **l'aggiornamento dello stesso in funzione degli interventi attivati** e **il conseguente dimensionamento/ridimensionamento dei Team**.

Utilizzando la suddivisione delle fasi in sprint, secondo il modello SCRUM, alla fine di ognuna è quindi possibile effettuare le seguenti attività in maniera trasparente, verificando costantemente l'andamento del progetto:

- **revisione pianificazione**: all'avvio di ogni sprint, è possibile valutare eventuali cambiamenti di scenario, aggiornare se necessario, le attività, ridefinendo, sulla base delle priorità e degli impatti le scadenze e i tempi per il completamento dello stesso. In presenza di impatti sulle Deliverable finali e in conseguenza di cambi di scenari dovuti a esplicite richieste del cliente, la revisione sarà concordata direttamente con l'Amministrazione che avrà chiaramente la piena visibilità del piano e del suo avanzamento;
- **revisione staffing**: la **variazione dei requisiti** e modifica l'allocazione delle risorse, tenendo conto di: competenze disponibili, strategicità degli interventi e scadenze previste.

Questi change in corso d'opera potranno comportare l'**Aggiornamento Piano di Lavoro**: con l'adozione di una metodologia Agile che permette una più puntuale conoscenza del contesto, delle risorse e delle competenze è possibile gestire situazioni complesse e rispondere al cambiamento continuo attraverso la:

- **ridefinizione delle priorità interne** ai Team di Progetto già presenti in Amministrazione, al fine di ripianificare l'organizzazione e le attività;
- **valutazione dei Team di Progetto** che, sulla base delle priorità definite o delle specifiche esigenze, si riorganizza, con ulteriori risorse interne disponibili presso il costituito RTI.

Nella fase attuativa del Piano di Migrazione, le relative attività previste a piano saranno successivamente monitorate e controllate secondo le modalità descritte in maniera dettagliata nel paragrafo **Errore. L 'origine riferimento non è stata trovata.** relativo all'ID 21.

## 22.3 Dimensionamento e Tempistiche per la Fase di Analisi/Discovery

La **fase di Analisi/Discovery** è, come già anticipato anche nel Progetto di Fattibilità, quella in cui si procede ad effettuare un assessment della PA, valutare il livello di maturità rispetto al Cloud, determinare la migliore strategia di migrazione e definire il piano di dettaglio della migrazione.

Secondo quanto riportato nello schema di convenzione le tempistiche previste per lo svolgimento di tali attività sono cadenzate nel seguente modo:

- entro **60 giorni** dalla ricezione del Piano dei Fabbisogni, il costituito RTI predisporrà il Progetto del Piano dei Fabbisogni contenente in particolare il **Piano di Migrazione di Massima**;

- entro **60 giorni** dalla stipula del Contratto, sarà predisposto **il Piano di Migrazione di Dettaglio**, redatto sulla base del Progetto del Piano dei Fabbisogni e del Piano di Migrazione di Massima contenente le attività e il piano temporale di dettaglio necessarie alla migrazione del Data Center dell'Amministrazione utente nel PSN.

Ai fini del dimensionamento/composizione del team mix e delle tempistiche di fase, il costituito RTI effettuerà la stima tenendo in considerazione le **seguenti variabili**:

1) **numerosità dei Rack oggetto di migrazione**, che classificano la dimensione dell'Amministrazione secondo i seguenti criteri:
    a) PA di piccole dimensioni: fino a 10 rack;
    b) PA di medie dimensioni: fino a 20 rack;
    c) PA di grandi dimensioni: oltre 20 rack;
2) **conoscenza del contesto della PA** da parte delle Società che fanno parte del costituito RTI;
3) **disponibilità e maturità della documentazione messa a disposizione dalla PA**: elementi riportati all'interno del Piano dei Fabbisogni presentato dall'Amministrazione (es. documenti preesistenti di assessment su livello di maturità del Cloud, documenti applicativi, disponibilità di un'Enterprise Architecture, catalogo servizi completo e maturo, etc.) o che dovessero emergere in sede di Kick-Off.

L'effettiva disponibilità di input documentali dell'Amministrazione, quali ad esempio la valutazione della cloud maturity corrente, o una descrizione puntuale delle architetture in uso, un Configuration Management DB aggiornato e completo etc., potranno, unitamente all'eventuale conoscenza da parte del costituito RTI della realtà IT in analisi, determinare la possibilità, in sede di pianificazione, di prevedere il completamento della fase di Analisi/Discovery in anticipo rispetto ai 60 giorni previsti dalla Convezione.

In virtù della significatività degli output di fase previsti, necessari per indirizzare le successive attività, il costituito RTI adotterà per ciascun scenario, **un team mix ad alta professionalità** che garantirà:

- completezza ed accuratezza dell'analisi del contesto tecnologico della PA;
- efficacia della progettazione della strategia di migrazione;
- tempestività nel completamento dell'analisi, al fine di garantire un pronto avvio della fase esecutiva.

| Team Mix per la fase di Analisi/Discovery | |
|---|---|
| **Macro Famiglia professionale** | **Figure Professionali di riferimento previste nel Progetto di Fattibilità** |
| Project Management | Project Manager, Technical Team Leader |
| Cloud Specialist e Architetti | Cloud Application Architect, Cloud Application Specialist, Cloud Security Specialist, Enterprise Architect |
| Database e Sistemisti | System Integrator & Testing Specialist, System and Network Administrator, Database Specialist and Administrator |

Di seguito si riporta l'approccio operativo previsto dal costituito RTI per l'applicazione del modello:

1. in funzione della **dimensione della PA in oggetto** (Grande, Media, Piccola) definita sulla base della **numerosità dei RACK oggetto di migrazione**, identificazione del **dimensionamento standard previsto**, ovvero delle giornate uomo previste del team mix previsto per la migrazione (gg/uu per PA Grande, gg/uu per PA Media e gg/uu PA Piccola);
2. valutazione dei **criteri aggiuntivi** relativi al livello di conoscenza del contesto dell'Amministrazione (High, Medium, Low, None) e della disponibilità e maturità della documentazione di riferimento fornita (High, Medium, Low, None);
3. determinazione del fattore correttivo rispetto al dimensionamento standard, rispetto ad una matrice di varianza.

**Esemplificativo**

| Criterio 1 | Livello | Delta vs Standard | Criterio 2 | Livello | Delta vs Standard |
|---|---|---|---|---|---|
| Conoscenza del Contesto Amministrazione | HIGH | -5% | Disponibilità e maturità documentazione | HIGH | -10% |
| | MEDIUM | 0% | | MEDIUM | 0% |
| | LOW | -2% | | LOW | 7% |

| | | | | | |
|---|---|---|---|---|---|
| | NONE | 5% | dell'Amministrazione | NONE | 10% |

4. applicazione del fattore correttivo e determinazione del dimensionamento previsto per la fase di Analisi/Discovery del progetto, come illustrato nella tabella successiva;

| **Amministrazione** | **1. Dimensione PA / Numero Rack** | **Dimensionamento Standard (Team Mix Migrazione x gg/uu stimate)** | **2. Conoscenza del Contesto Amministrazione (High /Medium/ Low/None )** | **3. Disponibilità e Maturità Documentazione PA (High /Medium/Low/None)** | **Fattore correttivo rispetto al Dimensionamento standard** | **Dimensionamento effettivo del progetto (Team Mix Migrazione x gg/uu stimate)** |
|---|---|---|---|---|---|---|
| Amministrazione 1 | Grande / Nr Rack | Tot. gg/uu standard per PA Grande | High | High | -x% | Tot. gg/uu per PA Amministrazione 1 |
| Amministrazione 2 | Media / Nr Rack | Tot. gg/uu standard per PA Media | Medium | Medium | -y% | Tot. gg/uu per PA Amministrazione 2 |
| Amministrazione 3 | Piccola / Nr Rack | Tot. gg/uu standard per PA Piccola | Low | Low | +k% | Tot. gg/uu per PA Amministrazione 3 |
| Amministrazione 4 | … | … | … | … | … | … |

In funzione dell'effettivo contesto dell'Amministrazione richiedente e di eventuali variabili specifiche rispetto all'ambito della PA, che dovessero presentarsi in corso di svolgimento delle attività, il costituito RTI, applicando le metodologie di dimensionamento e pianificazione descritte in precedenza, potrà rivedere team mix e dimensionamento al fine di adattarlo alle effettive esigenze e garantire il raggiungimento degli obiettivi previsti.

Questa metodologia di stima delle risorse necessarie, sebbene non possa che operare in range dimensionali rispetto a dimensioni predeterminate qui riportabili solo attraverso i casi d'uso esemplificativi, consentirà all'Amministrazione di avere riferimenti chiari e risposte certe agli impegni richiesti per la fase di migrazione, avendo casi d'uso cui confrontarsi come ordine di grandezza significativi.

## 22.4 Dimensionamento e Tempistiche per le Fasi di Setup/Migrazione/Collaudo

Il dimensionamento e la pianificazione delle fasi implementative della migrazione, ovvero quelle di Setup, Migrazione e Collaudo saranno strutturati tenendo in considerazione la strategia di migrazione individuata sulla base dei seguenti criteri:

- criteri previsti all'interno del Progetto di Fattibilità:
    - **numerosità dei Rack oggetto di migrazione**, che classificano la dimensione dell'Amministrazione secondo i seguenti criteri:
        - PA di piccole dimensioni: fino a 10 rack;
        - PA di medie dimensioni: fino a 20 rack;
        - PA di grandi dimensioni: oltre 20 rack.
    - **maturità dell'Amministrazione** in base al risultato del Cloud Maturity Model secondo il modello AgID *(0. Legacy, 1. Iniziale, 2. Opportunistico, 3. Sistematico, 4. Misurabile, 5. Ottimizzato)* e condiviso, in sede di assessment, con l'Amministrazione di riferimento.
- **criteri aggiuntivi e migliorativi proposti dal costituito RTI** nella realizzazione del modello che concorrano a determinare il livello di complessità del progetto di migrazione:
    - **conoscenza del contesto della PA** da parte delle Società costituenti il costituito RTI;
    - **disponibilità e Maturità della documentazione messa a disposizione dalla PA**: elementi riportati all'interno del Piano dei Fabbisogni presentato dall'Amministrazione (es. documenti preesistenti di assessment su livello di maturità del Cloud, documenti

applicativi, Enterprise Architecture, CMDB, etc.) o che dovessero emergere in sede di Kick-Off;

- **complessità dei servizi oggetto di migrazione**, emersa in fase di assessment; è infatti necessario considerare che oltre alla Cloud Maturity, sarà opportuno tenere in considerazione le variabili specifiche derivanti dal parco applicativo di quell'Amministrazione (es. pochi servizi con elevata complessità, cloud ready ma con presenza di servizi ad elevata complessità, etc.);
- **classificazione dei dati gestiti dalla PA**, secondo la metrica di ACN (dato ordinario, critico e strategico).

L'identificazione del livello di maturità di ciascuna PA, unita alla classificazione del dato e alla complessità dei servizi determina la scelta della (o delle) "landing zone" ovvero del mix ottimale di infrastrutture target definite nel Progetto di fattibilità: soluzioni Industry Standard (Housing, Hosting, Private Cloud), Hybrid Cloud on PSN site, Secure Public Cloud, Public Cloud PSN Managed. In un contesto progettuale in cui la metodologia prevalente per l'esecuzione delle migrazioni sarà quella Lift & Shift, il costituito RTI tuttavia non esclude la possibilità che in dipendenza del contesto specifico dell'Amministrazione si possano da subito sfruttare le funzionalità fornite dall'adozione di infrastrutture target Cloud-Native (Hybrid Cloud on PSN site, Secure Public Cloud, Public Cloud PSN Managed), senza intervenire in maniera sostanziale sul core delle Applicazioni.

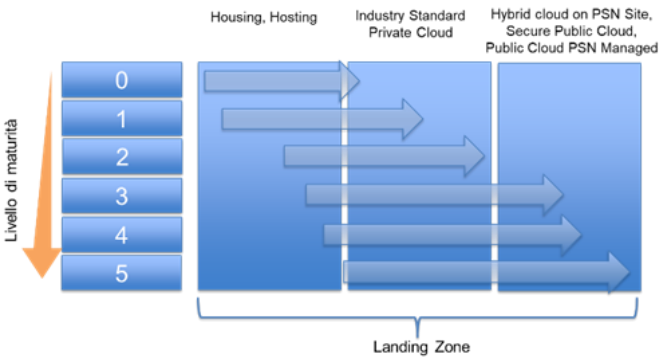



**Figura 34 Landing zone per livello di maturità**

Pertanto, il livello di maturità dell'Amministrazione rilevato nella fase di analisi non solo ha un impatto sull'effort di migrazione nel breve termine, ma determina l'evoluzione nel medio e nel lungo termine.
Si potranno quindi avere situazioni che presentano caratteristiche come quelle qui riportate a titolo esemplificativo:

- **amministrazione di dimensioni grandi** con dati classificati strategici e critici (oltre che ordinari) ma con un livello di maturità medio/alto, ad esempio 4, ovvero "misurabile", può effettuare una migrazione verso una configurazione ottimale che prevede un mix infrastrutturale costituito da ambienti Industry Standard (limitatamente al Private Cloud per i dati strategici), Hybrid Cloud on

PSN site, Secure Public Cloud per i dati critici e ordinari. In questo caso l'infrastruttura target, così come configurata a seguito della migrazione nel breve termine contiene già tutti gli elementi abilitanti per un successivo step che preveda anche la revisione delle architetture applicative in ottica re-platform e re-architect che può essere effettuata già nel medio termine;

- **amministrazione con livelli di maturità bassi**, il processo di trasformazione sarà più lungo, nel breve termine il re-hosting sarà finalizzato alla migrazione verso il PSN su infrastrutture quasi esclusivamente Industry Standard, ed il processo di evoluzione successiva verso soluzioni "cloud native" richiederà tempi maggiori e potrà essere realizzato solo nel medio e lungo termine. In questo ultimo caso il PSN potrà supportare l'evoluzione applicativa, che comporterà significative modifiche e riscritture delle applicazioni (re-architect), mettendo a disposizione gli strumenti e, se richiesto, tutti i servizi professionali a supporto del processo.

| | Dimensione PA | | |
|---|---|---|---|
| **Cloud Maturity** | Piccola | Media | Grande |
| 0 – Legacy | Media | Alta | Alta |
| 1 – Iniziale | Media | Media | Alta |
| 2 Opportunistico | Bassa | Media | Alta |
| 3 – Sistemistico | Bassa | Media | Media |
| 4 – Misurabile | Bassa | Bassa | Media |
| 5 -Ottimizzato | Bassa | Bassa | Bassa |

**Figura 35 Matrice di complessità**

L'applicazione dei criteri descritti in precedenza permette di definire **una matrice di complessità del progetto più articolata ed esaustiva dei possibili scenari progettuali** presenti nel progetto di fattibilità e che quindi consente una più efficace articolazione del dimensionamento del team mix e relative verifiche.

Le variabili aggiuntive, infatti, concorreranno a determinare dei fattori correttivi rispetto ad un team mix standard previsto per le complessità previste dal Progetto di Fattibilità (Alta, Media e Bassa).

Di seguito si riporta l'approccio operativo previsto dal il costituito RTI per l'applicazione del modello:

- **determinazione**, a partire dagli **output della fase di Analisi/Discovery** dell'Amministrazione, della **complessità del progetto** (Alta, Media, Bassa) funzione della Cloud Maturity dell'Amministrazione e della sua Dimensione**;**
- **identificazione**, in funzione della **strategia di migrazione**, del **dimensionamento standard**

**previsto**, ovvero delle giornate uomo previste per singola figura professionale del team mix (gg/uu per Progetto ad Alta Complessità, gg/uu per Progetto a Media complessità e gg/uu Progetto a Bassa Complessità);

- valutazione dei criteri aggiuntivi, relativi a: livello di conoscenza del contesto dell'Amministrazione (High, Medium, Low, None), disponibilità e maturità della documentazione di riferimento fornita (Alta, Media, Bassa, Nulla), complessità dei servizi oggetto di migrazione e classificazione dei dati gestiti dalla PA;
- determinazione del **fattore correttivo rispetto al dimensionamento standard**, rispetto ad un valore di riferimento standard:

**Esemplificativo**

| Criterio 3 | Livello | Delta vs Standard | Criterio 4 | Livello | Delta vs Standard |
|---|---|---|---|---|---|
| Conoscenza del contesto dell'Amministrazione | HIGH | -5% | Disponibilità e maturità documentazione dell'Amministrazione | HIGH | -10% |
| | MEDIUM | 0% | | MEDIUM | 0% |
| | LOW | -2% | | LOW | 7% |
| | NONE | 5% | | NONE | 10% |
| **Criterio 5** | **Livello** | **Delta vs Standard** | **Criterio 6** | **Livello** | **Delta vs Standard** |
| Complessità dei servizi oggetto di migrazione | HIGH | 15% | Classificazione dei dati gestiti dalla PA | HIGH | 10% |
| | MEDIUM | 0% | | MEDIUM | 0% |
| | LOW | -2% | | LOW | -3% |
| | NONE | -15% | | NONE | -10% |

- applicazione del fattore correttivo e determinazione del dimensionamento effettivo per le fasi di

Setup/Migrazione/Collaudo del progetto, come rappresentato in tabella:

| Amministrazione | Dimensione PA / Nr Rack | Cloud Maturity | Complessità del progetto | Strategia di migrazione | Dimensionamento Standard (Team Mix Migrazione x gg/uu stimate) | Fattore correttivo rispetto al Dimensiona-mento standard | Dimensionamento effettivo del progetto (Team Mix Migrazione x gg/uu stimate) |
|---|---|---|---|---|---|---|---|
| Amministrazione 1 | Grande / Nr Rack | 0. Legacy | Alta | Lift&Shift (Breve Termine) | Tot. gg/uu standard per Lift & Shift ad Alta complessità | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Tot. gg/uu per PA Amministrazione 1 |
| Amministrazione 2 | Media / Nr Rack | 1. Iniziale | Media | Lift&Shift (Breve Termine) | Tot. gg/uu standard per Lift & Shift a Media complessità | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Tot. gg/uu per PA Amministrazione 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Amministrazione 3 | Piccola / Nr Rack | 2. Opportunistico | Bassa | Lift&Shift (Breve Termine) | Tot. gg/uu standard per Lift & Shift a Bassa complessità | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Tot. gg/uu per PA Amministrazione 3 |
| Amministrazione 4 | Media / Nr Rack | 1. Iniziale | Media | Cloud Enabling (Medio/ Lungo Termine) | Tot. gg/uu standard per Lift & Shift a Media complessità | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Tot. gg/uu per PA Amministrazione 2 |

Il costituito RTI adotterà per ciascun scenario di migrazione, **un team mix ad alta professionalità** che garantirà:

- completezza ed accuratezza della fase di configurazione dell'infrastruttura;
- tempestività ed accuratezza della migrazione della PA;
- efficacia e completezza dei collaudi.

| **Team Mix per le fasi di Setup/Migrazione/Collaudo** | | **Ripartizione % gg/uu per fase di progetto** | | |
|---|---|---|---|---|
| **Macro Famiglia professionale** | **Figure Professionali di riferimento previste nel Progetto di Fattibilità** | **% Setup (gg/uu)** | **% Migrazione (gg/uu)** | **% Collaudo (gg/uu)** |

| | | | | |
|---|---|---|---|---|
| Project Management | Project Manager, Technical Team Leader | 32% | 34% | 34% |
| Cloud Specialist e Architetti | Cloud Application Architect, Cloud Application Specialist, Cloud Security Specialist, Enterprise Architect | 20% | 45% | 35% |
| Database e Sistemisti | System Integrator & Testing Specialist, System and Network Administrator, Database Specialist and Administrator | 35% | 35% | 30% |

In virtù delle eventuali peculiarità di ciascuna Amministrazione sarà poi possibile effettuare specifici tailoring od integrazioni, valutando anche l'attivazione dei Servizi Professionali ove sia necessario integrare nel Team Mix specifiche competenze (es. Sicurezza).

L'approccio descritto in relazione al dimensionamento abilita in particolare:

- la **verificabilità** da parte dell'Amministrazione dei razionali adottati da parte del costituito RTI per la stima dell'effort necessario per lo svolgimento del progetto di migrazione;
- il **continuous improvement** del modello, in funzione della possibilità a seguito del completamento di una determinata progettualità di valutare l'allineamento tra effort previsto ed effort effettivamente erogato, effettuando un fine tuning sui team mix.

Ai fini della **pianificazione dell'elapsed del progetto di migrazione**, saranno applicate le medesime logiche applicate per il dimensionamento al fine di determinare dei range standard di elapsed per ciascuna fase, secondo lo schema di seguito riportato:

| Amministrazione | Strategia di migrazione | Complessità del progetto | Elapsed standard per tipologia di progetto | Fattore correttivo rispetto all'elapsed standard | Elapsed stimato del progetto |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Amministrazione 1 | Lift&Shift (Breve Termine) | Alta | Elapsed medio per ciascuna fase (Setup, Migrazione, Collaudo) | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Elapsed previsto per PA Amministrazione 1 |
| Amministrazione 2 | Lift&Shift (Breve Termine) | Media | Elapsed medio per ciascuna fase (Setup, Migrazione, Collaudo) | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Elapsed previsto per PA Amministrazione 2 |
| Amministrazione 3 | Lift&Shift (Breve Termine) | Bassa | Elapsed medio per ciascuna fase (Setup, Migrazione, Collaudo) | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Elapsed previsto per PA Amministrazione 3 |
| Amministrazione 4 | Cloud Enabling (Medio/ Lungo Termine) | Media | Elapsed medio per ciascuna fase (Setup, Migrazione, Collaudo) | % di incremento / decremento in funzione dell'applicazione dei fattori correttivi | Elapsed previsto per PA Amministrazione 4 |

## 22.5 Use Case

Al fine di fornire un'applicazione concreta dell'approccio metodologico relativo al dimensionamento e pianificazione di un progetto di migrazione, il costituito RTI in sede di Offerta Tecnica, in virtù della consolidata esperienza in ambito migrazione dalle Società rappresentanti (TIM, Leonardo e Sogei), è già in grado di presentare dei casi d'uso dell'applicazione del modello, che rappresentano esempi di esperienze progettuali.

Nello specifico sono presentati **3 Use Case** che rappresentano le seguenti casistiche[6]:

[6] Vedi nota 1 al capitolo 1 "Executive Summary". I casi d'uso per i motivi lì riportati non riguardano il cloud enabling considerando i maggiori impatti rispetto all'estrema complessità e variabilità delle dimensioni considerate nel modello per questa tipologia di interventi.

- **Use Case 1 "Best Case":** progetto a bassa complessità (nr di rack limitati) con variabili di contesto migliorative (es. profonda conoscenza dell'Amministrazione, disponibilità di documentazione, etc.);
- **Use Case 2 "Worst Case":** progetto ad alta complessità (nr di rack elevati e livello di cloud maturity iniziale) con variabili di contesto peggiorative (es. limitata conoscenza dell'Amministrazione, assenza di documentazione, servizi da migrare complessi, etc.);
- **Use Case 3 "Mixed Case":** progetto a media complessità (nr di rack intermedio e livello di cloud maturity intermedio) con variabili di contesto migliorativi (servizi da migrare a bassa complessità) e peggiorative (es. conoscenza nulla dell'Amministrazione, assenza di documentazione).

### 22.5.1 Use Case 1 – "Best Case"

Lo scenario prevede i seguenti elementi caratterizzanti:

| Amministrazione | Dimensione PA | Cloud Maturity | Complessità del progetto | Strategia di migrazione | Conoscenza del contesto dell'Amministrazione | Disponibilità e maturità documentazione dell'Amministrazione | Complessità dei servizi oggetto di migrazione | Dati Gestiti |
|---|---|---|---|---|---|---|---|---|
| Amministrazione 1 | Piccola | 2. Opportunistico | Bassa | Lift&Shift (Breve Termine) | High | High | Low | Ordinari |

In funzione di tali parametri si determina il fattore correttivo (in questo caso migliorativo) rispetto ad un progetto standard di riferimento sia in termini di gg/uu sia in termini di elapsed di fase:

| Dimensionamento e Pianificazione | Totale | Analisi | Setup | Migrazione | Collaudo |
|---|---|---|---|---|---|
| **Dimensionamento del progetto gg/uu** | **750** | 220 | 145 | 315 | 70 |

| | | | | | |
|---|---|---|---|---|---|
| **Elapsed** | **130 giorni** | 60 giorni | 20 giorni | 40 giorni | 10 giorni |

### 22.5.2 Use Case 2 – "Worst Case"

Lo scenario prevede i seguenti elementi caratterizzanti:

| Amministrazione | Dimensione PA | Cloud Maturity | Complessità del progetto | Strategia di migrazione | Conoscenza del contesto dell'Amministrazione | Disponibilità e maturità documentazione dell'Amministrazione | Complessità dei servizi oggetto di migrazione | Dati Gestiti |
|---|---|---|---|---|---|---|---|---|
| Amministrazione 2 | Grande | 0. Legacy | Alta | Lift&Shift (Breve Termine) | None | None | High | Strategici e Critici |

In funzione di tali parametri si determina il fattore correttivo (in questo caso peggiorativo) rispetto ad un progetto standard di riferimento sia in termini di gg/uu sia in termini di elapsed di fase:

| Dimensionamento e Pianificazione | Totale | Analisi | Setup | Migrazione | Collaudo |
|---|---|---|---|---|---|
| **Dimensionamento del progetto gg/uu** | **5.260** | 1.540 | 1.000 | 2.200 | 520 |
| **Elapsed** | **310 giorni** | 120 giorni | 50 giorni | 110 giorni | 30 giorni |

### 22.5.3 Use Case 3 – "Mixed Case"

Lo scenario prevede i seguenti elementi caratterizzanti:

| Amministrazione | Dimensione PA | Cloud Maturity | Complessità del progetto | Strategia di migrazione | Conoscenza del contesto dell'Amministrazione | Disponibilità e maturità documentazione dell'Amministrazione | Complessità dei servizi oggetto di migrazione | Dati Gestiti |
|---|---|---|---|---|---|---|---|---|
| Amministrazione 3 | Media | 3. Sistemistico | Media | Lift&Shift (Breve Termine) | None | Low | Low | Presenza dati CRITICI |

In funzione di tali parametri si determina il fattore correttivo rispetto ad un progetto standard di riferimento sia in termini di gg/uu sia in termini di elapsed di fase:

| Dimensionamento e Pianificazione | Totale | Analisi | Setup | Migrazione | Collaudo |
|---|---|---|---|---|---|
| **Dimensionamento del progetto gg/uu** | **2.920** | 850 | 560 | 1.220 | 290 |
| **Elapsed** | **220 giorni** | 100 giorni | 30 giorni | 70 giorni | 20 giorni |

## 22.6 Approccio metodologico per l'esecuzione delle fasi di Migrazione




Per la gestione operativa della migrazione, il costituito RTI prevede di utilizzare un framework metodologico proprietario **EMG2C** (**Explore, Make, Go to Cloud**) (Figura 36) che consente di guidare tutte le fasi di un progetto di migrazione verso il cloud e delle sue successive evoluzioni, sfruttando le best practice delle metodologie e dei modelli rappresentati in figura e che ha la capacità di dimensionare le risorse necessarie alla migrazione. Inoltre, mette a disposizione strumenti e template che permettono di implementare una gestione completa di ogni fase.

Parte integrante del framework sono le Best Practice di ambito tecnologico che rappresentano il corretto approccio metodologico per obiettivi tecnologici, fornite direttamente dai produttori (Microsoft, Oracle, Google, VMware).

Le fasi principali del framework sono Explore, Make e Go:

- **Explore** include le fasi relative all'analisi e alla valutazione dell'ambiente, per aiutare la PA a definire il proprio percorso di migrazione verso il cloud. In questa fase si valuterà il livello attuale di adozione al Cloud dell'ente attraverso il Cloud Maturity Model, l'attuale postura in termini di sicurezza attraverso l'uso di analisi DAST e VA e saranno raccolte tutte le informazioni relative alle componenti da migrare;
- **Make** è la fase che comprende tutte le attività di design e di predisposizione dell'ambiente per permettere la migrazione in condizioni di sicurezza, tra cui anche i test necessari a validare il disegno di progetto. È in questo step che si valuta la migrazione one shot oppure in più wave, a seconda del grado di complessità o gli SLA di servizio dell'ambiente di partenza. Nel caso della migrazione verso il PSN, sono stati considerati **due step principali: Setup e Migrazione**;
- **Go** è la fase finale del processo che prevede il collaudo, l'attivazione dei servizi sulla nuova infrastruttura ed anche le attività di post go live necessarie al supporto e all'ottimizzazione dei servizi nel nuovo ambiente.

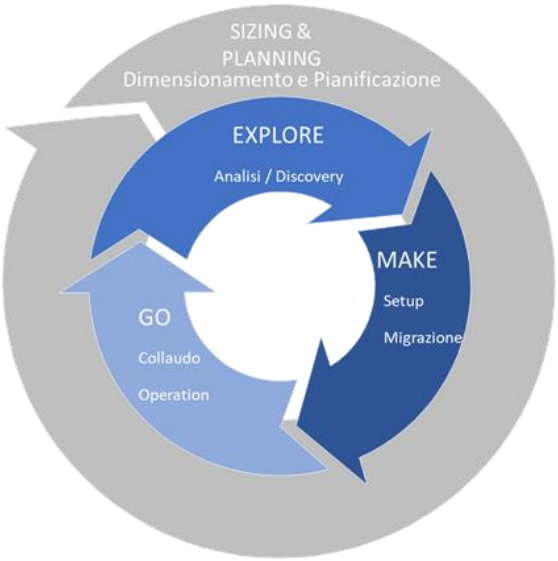



**Figura 36 Framework metodologico**

Il framework, quindi, permette di gestire tutte le fasi della migrazione, dall'analisi alla progettazione, alla realizzazione e al monitoraggio della messa in produzione e della successiva fase di post-produzione e costituisce il modello metodologico del costituito RTI per le attività di migrazione.

Ogni step del framework è in grado di rispondere alle diverse richieste che si possono presentare e può essere suddiviso in sottofasi la cui complessità e durata è chiaramente dipendente dall'ambiente da migrare. A questo proposito il framework permette di utilizzare approcci di **tipo Waterfall** o di **tipo Agile** a seconda della numerosità e delle tipologie delle architetture esistenti e di conseguenza degli interventi richiesti per mettere in pratica le strategie di migrazione.

Nel caso, infatti di una strategia di tipo **Retain**, in cui non si prevede alcuna trasformazione e per cui il

servizio richiesto al PSN è un Housing, **l'approccio di tipo Waterfall** presenta il vantaggio di pilotare al meglio lo spostamento delle infrastrutture verso il PSN, utilizzando una sequenza di attività, consolidate dall'esperienza delle Società costituenti il costituito RTI.

Nel caso invece di una **strategia di tipo Lift&Shift**, in cui le variabili e il grado di complessità dipendono da molteplici fattori, tra cui anche il livello di importanza del dato stesso, **l'approccio di tipo Agile SCRUM** risulta più indicato, in quanto in grado di conformarsi sulle specifiche esigenze di progetto proprio per sua natura. SCRUM è infatti un framework che aiuta a creare valore attraverso un percorso di adattamento alle attività complesse. Ogni obiettivo viene suddiviso in fasi temporalmente limitate, i cosiddetti sprint, con obiettivi più facilmente misurabili e quindi che consentono di migliorare il controllo degli avanzamenti e di evidenziare ed affrontare rapidamente le criticità che potrebbero sorgere durante il progresso del progetto.

Come rappresentato all'interno del Progetto di Fattibilità, ciascun progetto di Migrazione è articolato nelle seguenti fasi:

**EXPLORE** 

1. **Analisi/Discovery:** fase di assessment della Amministrazione target e definizione della strategia di migrazione, che persegue i seguenti principali obiettivi:
   1.1. identificare il livello di maturità del Cloud della PA ed i gap rispetto al livello atteso, al fine di rispettare gli obiettivi del PNRR. Il livello sarà misurato seguendo gli indirizzi definiti da AgID con Cloud Maturity Model e le linee guida per l'abilitazione al cloud. A questi fattori, già definiti nel Progetto di Fattibilità come condizione migliorativa ed alla luce delle recenti norme di classificazione dei dati delle Amministrazioni, saranno aggiunti due gradi di complessità dati dalla **classificazione dei dati** da migrare (*secondo la recente determina n. 306 dell'Agenzia per la Cybersicurezza sul modello per la predisposizione dell'elenco e della classificazione di dati e di servizi*) e dalla **complessità architetturale delle soluzioni** in particolare per quelle a minor grado di maturità cloud;
   1.2. raccogliere tutte le informazioni relative alla infrastruttura e ai workload da migrare;
   1.3. supportare ove necessario **l'amministrazione per la classificazione dei dati e servizi** secondo il modello della strategia Cloud Italia e le regole emanate da ACN;

1.4. definire, in base alle evidenze emerse, la strategia di migrazione rispetto alle possibili soluzioni (Housing, Hosting, Private Cloud (IaaS e PaaS), etc.);

1.5. definire il piano di dettaglio della migrazione della PA;

**MAKE** 

2. **Setup:** fase di progettazione esecutiva della strategia di migrazione individuata finalizzata a:

   2.1. mappare i servizi e le infrastrutture in uso alla singola amministrazione sui servizi offerti dal PSN;

   2.2. predisporre l'infrastruttura target presso i nuovi DC, in termini di workload ed architettura logica/fisica, al fine di abilitare l'effettiva migrazione della PA;

3. **Migrazione:** fase realizzativa in cui si realizza la strategia di migrazione individuata attraverso l'effettiva movimentazione dei dati, l'implementazione delle policy di sicurezza e l'implementazione del monitoraggio dell'infrastruttura;

**GO** 

1. **Collaudo:** fase conclusiva del piano di migrazione, volta a certificare la corretta migrazione dell'infrastruttura e finalizzato a testare le procedure e modalità della migrazione;

2. **Operation:** a seguito del collaudo funzionale della intera infrastruttura di ogni PA, il costituito RTI erogherà tutti i Servizi di gestione richiesti dalla PA.

All'interno dei successivi paragrafi per ciascuna fase, è esplicitato l'approccio metodologico che sarà adottato dal costituito RTI per uno specifico progetto di migrazione.




| | | | | |
|---|---|---|---|---|
| Step 1 | Assessment | Predisposizione e Configurazione Ambienti | Esecuzione Migrazione | Definizione Strategia di Collaudo |
| Step 2 | Definizione Strategia di Migrazione | | | Esecuzione Collaudo e reporting |
| Step 3 | Progettazione e Pianificazione Migrazione | | | |

**Figura 37 Approccio metodologico**

### 22.6.1 EXPLORE - Fase di Analisi/Discovery

La fase di Analisi/Discovery rappresenta l'avvio del percorso di abilitazione al Cloud e prevede **i seguenti step operativi**:

1. **Assessment:** l'obiettivo di questo step è l'identificazione del **"footprint" applicativo** e **tecnologico AS-IS** dell'Amministrazione e la definizione di una **base di conoscenza condivisa** tra tutti gli stakeholder coinvolti. Nel corso dell'assessment il costituito RTI acquisirà informazioni in relazione ai seguenti ambiti:
    - **Business:** si raccolgono informazioni rispetto ai requisiti e ai fabbisogni strategici espressi dall'Amministrazione al fine di indirizzare correttamente la definizione della strategia di Cloud Migration;
    - **Organization**: si raccolgono dati e informazioni inerenti al modello organizzativo e operativo in essere, i processi di business e i processi IT con l'obiettivo di contestualizzare le varie applicazioni in uso, nonché indirizzare la successiva definizione del nuovo modello operativo IT;
    - **Technology:** si raccolgono e analizzano i dati necessari alla comprensione e alla definizione del portfolio applicativo e del footprint infrastrutturale della singola PA;
    - **Complexity:** le informazioni raccolte sono catalogate anche secondo questa dimensione in modo da tenere conto della classificazione dei dati e la complessità architetturale dei servizi;
    - **Security & Risk Management:** si valutano impatti e requisiti/vincoli normativi previsti per le PA in termini di sicurezza e fondamentali per la definizione del perimetro di intervento nonché per la prioritizzazione degli applicativi da migrare in Cloud.

    A valle, i dati ed i servizi gestiti dall'Amministrazione saranno classificati secondo il modello individuato dall'Agenzia per la Cybersicurezza nazionale:

    - **strategico:** dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
    - **critico:** dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;
    - **ordinario:** dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

2. **Definizione Strategia di Migrazione:** l'obiettivo è supportare le Amministrazioni nella definizione della strategia di migrazione dei propri sistemi in Cloud; la priorità di traguardare, in primis, lo spostamento del perimetro complessivo dei servizi dell'Amministrazione all'interno dell'infrastruttura del PSN, sarà bilanciata comunque con la valutazione di elementi a contorno che possano determinare, già in questa fase una trasformazione verso il cloud, al fine, ove possibile e di concerto con l'Amministrazione stessa, di facilitare comunque gli step successivi di evoluzione digitale.

   Sulla base delle informazioni catalogate durante lo step di Assessment e tenendo presente che una delle finalità primarie è velocizzare da un lato la chiusura dei CED delle Amministrazioni e dall'altro far evolvere i servizi in ottica digitale e cloud, si valuteranno i seguenti aspetti:

   - esistenza di progetti già pronti o in via di completamento e volontà dell'Amministrazione di migrare o meno i servizi verso il nuovo paradigma già definito. Questo elemento seppur potendo influire sul processo di migrazione facendo intervenire operazioni di medio/lungo termine, ne faciliterà in assoluto la trasformazione ed i costi che comporta, consentendo di utilizzare la nuova infrastruttura PSN, più evoluta, da subito come target del progetto già definito di trasformazione;
   - limitazione per quanto più possibile di soluzioni di housing ed hosting, per quei servizi per cui si rilevi che a fronte di minimi interventi si possa procedere comunque alla virtualizzazione, favorendo così la loro successiva trasformazione e re-architect, nonché l'uso di servizi del PSN a maggiore efficienza ottimizzati anche nei costi.

   Quindi, pur considerando che l'attesa è per un approccio molto diffuso di una migrazione lift & shift nel breve termine, si pongono da subito le condizioni, ove possibile e valutato congruo dall'Amministrazione, per gli step successivi di trasformazione. La strategia di Migrazione, tenendo in considerazione il livello di maturità del Cloud dell'Amministrazione valutato nella fase di Assessment, si baserà principalmente su un approccio a breve termine, senza trascurare i possibili ambiti di intervento a medio e lungo termine per i casi che si possano presentare come di maggior probabilità di successo in piena sicurezza.

   In ogni caso, per le fasi successive il PSN, ha le competenze e capacità per le evoluzioni necessarie per una completa Cloud Transformation, che saranno però basate su scelte dell'Amministrazioni in termini di tempi modi e livello di ingaggio del PSN stesso per la loro progettazione e realizzazione. Questo non escluderà, come detto, analisi specifiche che

portino alla mappatura dei vari ambienti e delle migliori soluzioni offerte dal PSN per rispondere allo stato di maturità trovato e che prenderà in considerazione, d'accordo con l'Amministrazione, gli interventi ritenuti indispensabili per assicurare: funzionamento e sicurezza delle soluzioni una volta migrate[7].

3. **Progettazione e Pianificazione della Migrazione:** il cui obiettivo è declinare la strategia di migrazione definita e validata dall'Amministrazione in una progettazione di alto livello della architettura target ed in un piano operativo che permetta di traguardare gli obiettivi previsti, definendo attività, responsabilità, dipendenze, etc.

Sono di seguito approfonditi obiettivi e attività previste da ciascun step:

### Step 1.1 | Assessment - Data Collection & Analysis

Tenendo conto della metodologia di misurazione della complessità dell'Amministrazione da migrare, nel corso dell'Assessment si raccoglieranno tutte le informazioni che consentiranno di cogliere gli elementi fondamentali su servizi ed infrastrutture coinvolte indipendentemente se poi si potranno o meno applicare sin da subito nella fase di migrazione, tutti gli step tipici del modello di trasformazione cloud e delle Best Practices AgID in merito.




**Figura 38 Step 1 - Assessment**

La metodologia descritta sarà oggetto di tailoring da parte del costituito RTI in funzione delle evidenze relative all'Amministrazione, le quali potrebbero determinare un perimetro di attività più ridotto rispetto a quanto proposto *(ad esempio la prioritizzazione dei servizi da migrare potrebbe non essere considerato in ambito per l'Amministrazione, in quanto la migrazione potrebbe essere slegata ad una trasformazione o ridisegno architetturale)*. Il costituito RTI applicherà, comunque, alcuni approfondimenti tipici di questo processo in quanto ritiene che adottare un approccio così strutturato, non solo faciliterà l'onboarding dell'Amministrazione sul PSN dando un valore alla migrazione, ma potrà fornire valore anche ai successivi step. Questo step di analisi, infatti, rappresenterà un patrimonio da capitalizzare per la

[7] Il livello minimo di configurazione, di versioning dei prodotti, alcuni elementi anche applicativi (es. IP scolpito nelle applicazioni) che consentano anche attraverso l'opera di Lift&Shift di garantire, con piccoli interventi, sin da subito un'ambiente stabile e sicuro al miglior livello di virtualizzazione/cloud per facilitare la gestibilità ed il funzionamento dei servizi nel nuovo ambiente, facilitando gli step di evoluzione successivi.

completa trasformazione dei servizi dell'Amministrazione, indipendentemente che l'effettivo progetto realizzativo sia eseguito dal costituito RTI.

In particolare, nello step di Assessment, l'attività di **Data collection** ha lo scopo di raccogliere, identificare, documentare, tracciare e validare dati relativi al contesto dell'Amministrazione per creare un set informativo univoco che faciliti la definizione di ognuno di questi punti. In primo luogo, il costituito RTI analizza le informazioni eventualmente già disponibili (es. documentazione allegata al Piano dei Fabbisogni dell'Amministrazione) e, successivamente, si attiva per raccogliere dati e informazioni secondo approcci diversi:

- **survey per la raccolta dati**, mediante compilazione di template strutturati, realizzati ed inviati dal costituito RTI, da parte degli stakeholder della PA. Questa modalità si applica in funzione della tipologia di servizi e applicazioni che rientrano nell'intervento. Gli stakeholder a cui sottoporre la survey vengono condivisi con l'Amministrazione e i template messi a disposizione sul Portale. I template saranno costruiti sull'esperienza delle tre Società che compongono il costituito RTI e rappresenteranno, sia un primo metodo di razionalizzazione delle informazioni, sia la base dei successivi approfondimenti specifici;
- **interviste one-to-one** con i referenti dell'Amministrazione per la raccolta di dati inerenti tutti i driver di analisi e, in particolare, per il driver "Technology" al fine di raccogliere informazioni relative alle applicazioni che sono considerate critiche dall'Amministrazione stessa anche in termini, come già detto, di eventuali processi maturi per la trasformazione degli stessi ove possano essere d'intesse sin dalla fase di migrazione. Il Team di Progetto definirà d'accordo con l'Amministrazione un calendario di interviste e quali referenti coinvolgere: allo stesso modo verrà valutato e condiviso il coinvolgimento di altri Fornitori già impegnati presso la PA nella gestione di servizi e/o applicativi. Tutte le interviste saranno supportate dall'adozione di strumenti quali template, modelli e checklist sviluppati dal costituito RTI per la Fornitura e disponibili nell'area riservata del Portale della Fornitura;
- **document repository** ossia raccolta di tutta la documentazione disponibile presso la PA per ciascuno dei driver del framework.

Per la conduzione delle attività di Data Collection, il costituito RTI si avvale di alcune specifiche metodologie:

- **metodologia di Application Portfolio Assessment ed Enterprise Architecture**. Tale metodologia fornisce un approccio operativo per l'Assessment del portfolio applicativo e

consente di effettuare un'analisi a 360° di ciascuna applicazione, rappresentando le informazioni raccolte secondo una logica di architettura enterprise. L'Assessment prende in considerazione diversi parametri che consentono di misurare e valutare la condizione tecnologica dell'applicazione, la sua adeguatezza nel supportare i processi dell'Amministrazione e la spesa sostenuta per la sua realizzazione, evoluzione e manutenzione. Accanto alla componente applicativa vi è la componente metodologica di Enterprise Architecture Framework: ispirata ai principi fondamentali della metodologia TOGAF, può essere facilmente adattata al contesto e alle esigenze della specifica PA trattandosi di un approccio modulare, flessibile, innovativo e scalabile che abilita la creazione di valore tramite l'allineamento delle "capability" del Business e dell'IT, tenendo conto dei diversi domini e driver di analisi. Ove l'Amministrazione disponesse di un'EA matura e supportata da strumenti che ne consentano la navigazione e l'analisi 'informatica, questo avrà un impatto nella riduzione dei tempi e dell'impegno relativo alla fase di Analisi/Discovery;

- **metodologia di Software Licensing & Asset Management.** Il Framework SAM (Software & Licensing Asset Management)**,** conforme ai principali standard di riferimento in ambito IT Asset Management (es. ISO 19770), si articola in tre livelli**:**
    - **governance,** definisce il perimetro e gli obiettivi del SAM. La governance è uno degli elementi chiave nella gestione degli asset IT perché in grado di abilitare azioni di riduzione dei costi e mitigazione dei rischi di non conformità grazie a competenze specifiche e strumenti innovativi;
    - **gestione,** presidia l'ottimizzazione dei processi di gestione fabbisogni e i rinnovi contrattuali nonché l'attività di riconciliazione delle licenze;
    - **operatività,** presidia l'ottimizzazione degli strumenti di monitoraggio dei processi di inventariazione e riconciliazione delle licenze e l'integrazione con il ciclo di vita degli asset software;
- metodologia di **Cyber Security Assessment** Tale metodologia consente di identificare il livello di maturità di sicurezza informatica AS-IS della PA. L'approccio prevede l'analisi di tre dimensioni: **Governance, Detection e Prevention**. Ciascuna è costituita da diversi domini di sicurezza e aree correlate: vengono in tal modo identificate potenziali lacune e impatti su **Organizzazione, Processi e Tecnologia** al fine ultimo di definire le opportune "*remediation activities*"; sarà inoltre anche valutata l'attuale postura in termini di sicurezza applicativa e infrastrutturale attraverso l'uso di analisi DAST (Dynamic Analysis Security Testing) e VA (Vulnerability Assessment)

effettuati verso le applicazioni esistenti nella PA richiedente.

A valle della raccolta dati sul contesto AS-IS della PA, è attivata **la fase di Data Analysis** ovvero una fase di analisi e rielaborazione di quanto emerso sino alla redazione di tre deliverable - **Lista degli Applicativi, Mappatura Applicativa e Documento di Assessment** –. I risultati dell'analisi vengono discussi con i referenti dell'Amministrazione al fine di rilevare ogni potenziale opportunità, dipendenza o vincolo da tenere in considerazione nella fase successiva di valutazione del grado di maturità degli applicativi rispetto all'adozione del paradigma Cloud oltre che nella successiva attività di definizione della strategia di migrazione.

### Step 1.2 | Assessment – Misurazione della Cloud Maturity

L'obiettivo della fase è porre le basi per la definizione della strategia di migrazione dell'Amministrazione all'interno dell'infrastruttura PSN. Ciò è possibile in quanto le attività condotte nella fase abilitano:

- la **misurazione del livello di maturità al Cloud dell'Amministrazione**, valutato secondo criteri oggettivi e che determinano l'assegnazione alla singola Amministrazione di un livello di Cloud Maturity secondo la scala individuata nel Progetto di Fattibilità *(0. Legacy, 1. Iniziale, 2. Opportunistico, 3. Sistematico, 4. Misurabile, 5. Ottimizzato)*; il *grade* complessivo sarà costruito in modalità bottom-up, valutando **il livello di readiness delle applicazioni della PA** rispetto **all'adozione dei paradigmi Cloud**;
- la **classificazione** e la **prioritizzazione delle applicazioni**. La progressività delle attività (in caso di migrazione che non preveda esclusivamente un intervento Lift & Shift all'interno del PSN) consente in fase di esecuzione della migrazione di sfruttare i **benefici derivanti dalla curva di apprendimento**, **riutilizzando le ulteriori competenze acquisite e affinando le procedure operative** e riducendo così l'effort necessario oltre che i potenziali rischi o criticità.

**In funzione dei dati di input e di un algoritmo di valutazione** che tenga conto anche della complessità delle applicazioni legacy, la metodologia permette di associare **un punteggio alle applicazioni**, prendendo in considerazione **la readiness alla migrazione in Cloud**, e una **priorità**. Di seguito le attività in cui si articola la metodologia:

- definizione e calcolo del modello e dei criteri per la valutazione del livello di Readiness delle applicazioni; il modello per il calcolo dell'Application Readiness è costruito sulla base di attributi appartenenti alle categorie: Business Alignment, Application Architecture, Infrastructure

Architecture e Risk & Regulatory. Sulla base di razionali e criteri puntuali, permette di definire in riferimento a ogni attributo se la specifica applicazione risulta essere: Pronta, Neutrale o Non Pronta rispetto al paradigma Cloud:

  - architettura applicativa;
  - criticità dell'applicazione;
  - requisiti di availability dell'applicazione;
  - livello di dipendenza dell'infrastruttura sottostante;
  - linguaggio di programmazione;
  - compatibilità con il Cloud del sistema operativo;
  - tipologia di dati trattati dall'applicazione;
  - frequenza e metodologia dei rilasci;
  - stack SW utilizzato;
  - tecniche di integrazione;
  - manutenibilità del SW;
  - tipologia servizi erogati;
  - infrastruttura di erogazione;

- dalla valutazione del valore di readiness delle singole applicazioni, sarà poi determinato il livello complessivo di maturità dell'Amministrazione secondo la scala definita all'interno del Progetto di Fattibilità;
- **definizione del livello di priorità a ciascuna applicazione**; l'approccio prevede di assegnare la **priorità di migrazione in Cloud** *(tale priorità potrà essere funzionale nella pianificazione delle attività qualora il progetto di migrazione non preveda una soluzione di tipo Lift & Shift quale Housing / Hosting all'interno del PSN)*, in funzione di un albero decisionale guidato dai seguenti driver:

  - **valore di readiness dell'Applicazione** (Pronta, Neutra, Non Pronta); le applicazioni che risultano essere non pronte hanno un livello di priorità inferiore rispetto alle altre;
  - **opportunità da cogliere**: le applicazioni da analizzare in modo prioritario in vista della migrazione in Cloud sono quelle a cui è associata elevata opportunità di benefici, soprattutto economici, (in termini di riduzione dei costi);
  - rischio migrazione: le applicazioni devono essere valutate in termini di rischio connesso alla migrazione basato sugli eventuali impatti sulla continuità del servizio; sono da considerare prioritarie le applicazioni caratterizzate da un basso rischio;

- **semplicità migrazione**: le applicazioni devono essere valutate in termini di **facilità delle attività operative di migrazione** in Cloud. Sono da considerare prioritarie **le applicazioni** caratterizzate da **elevata semplicità di migrazione**;

- l'alberatura alla base del framework consente, quindi, di assegnare un livello di priorità alle applicazioni compreso tra **1 e 9, dove la priorità massima è pari a 1 e la priorità minima è pari a 9**. Le Applicazioni aventi un valore di readiness pari a "Pronta"/"Neutrale" sono poi valutate considerando i restanti parametri.

Come anticipato in precedenza, in considerazione che la finalità è l'onboarding completo dell'Amministrazione, anche delle applicazioni con un livello di maturità cloud basso o nullo, la definizione delle priorità delle migrazioni terrà conto anche per questa di fattori di semplicità/complessità in ambito legacy per definirne le priorità indipendentemente dall'ambito PSN target della migrazione (es. Housing, o hosting).

### Step 1.3 / Assessment - Classificazione dei dati e servizi dell'Amministrazione

La classificazione dei dati e dei servizi[8] è uno degli elementi alla base della Strategia Cloud Italia ed è un elemento complesso da realizzare, se non in presenza di una forte strutturazione nei processi IT e con competenze specifiche tecnico/organizzative relative alla Governance dati.

Considerando l'importanza di questa classificazione, sia per definire la complessità della migrazione, sia per le successive attività di cloud enabling che l'Amministrazione dovrà sostenere nel medio e lungo termine ove il CMM (Cloud Maturity Model) risulti al momento della migrazione, insufficiente per adottare subito servizi Cloud del PSN, il RTI propone all'Amministrazione che non avesse completato questa classificazione, la possibilità di accompagnarla in questa fase o, ove l'avesse già realizzata ma la volesse 'approfondire', i servizi necessari a realizzarla/completarla/validarla.

A seguire è rappresentato uno schema esemplificativo del contesto, che chiaramente è fortemente correlato alla fase di assessment finalizzata alla migrazione.

La raccolta delle informazioni relative ai dati e degli strumenti ad uso dell'amministrazione (cataloghi, EA, classificazione dati e correlazione tra servizi, etc.), consentirà anche di **definire la classe dei dati interessati alla migrazione**. Questa analisi, che sarà in ogni caso svolta per acquisire informazioni sulla

[8] La classificazione prevista dalla strategia Cloud Italia è direttamente riferita solo ai dati in quanto i servizi lo saranno indirettamente considerando cosa trattano.

tipologia di dati da migrare e sulla complessità conseguente della piattaforma di atterraggio della migrazione, consentirà di definire gli impatti sulla migrazione della classe dei dati di cui dispone l'Amministrazione.

La **gestione di dati strategici** comporta, infatti, una maggiore complessità nella migrazione che si dipana in tutte le fasi che la caratterizzano, dall'EXPLORE, al MAKE e sino al GO. Infatti, se sarà necessario approfondire la classificazione ove presente, o costruirla/finalizzarla nella fase di raccolta, la presenza di dati strategici influirà sulla profondità di informazioni da raccogliere; così come nella progettazione e realizzazione renderà più complesso il disegno della soluzione per la "landing zone" e per le modalità di interconnessione, controllo e sicurezza degli ambienti.

Questa analisi avverrà secondo **il modello previsto dalla strategia Cloud Italia** in modo da renderla indipendente da modalità non standard e non replicabili, tenendo anche conto che la classificazione dei dati riveste un aspetto dinamico che può portare a variazioni nel tempo della classe di servizi e dati. In questo modo si tratterà di un output a disposizione nel tempo dell'Amministrazione che può farla pienamente entrare nei propri processi evolutivi, nonché utilizzarla appieno nelle fasi di Cloud Enabling che seguiranno.

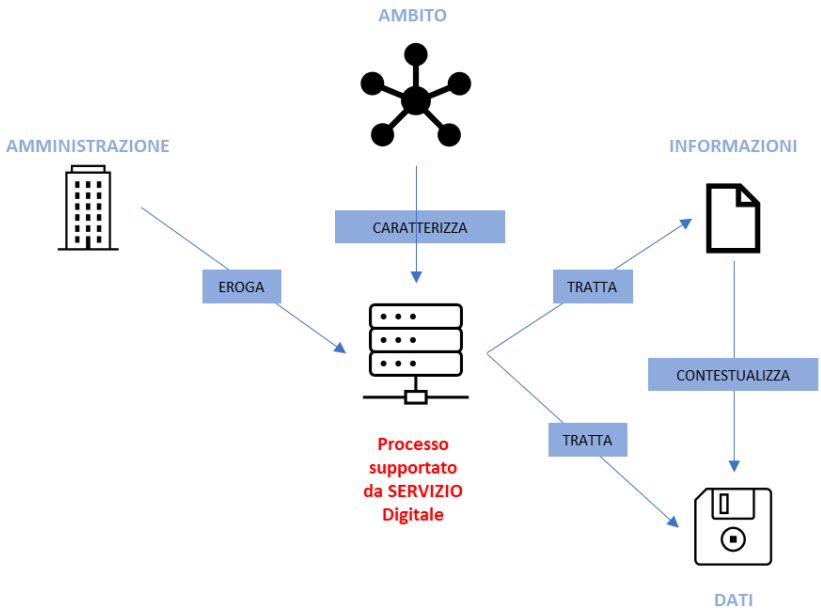



**Figura 39 Processo di classificazione dati e servizi digitali**

### Step 2 | Definizione Strategia di Migrazione




**Figura 40 Step 2 - Definizione Strategia di Migrazione**

La definizione della strategia di migrazione si compone delle seguenti due macro-attività:

- definizione Vision di Migrazione: attività di analisi degli obiettivi strategici e IT della PA finalizzata a delineare i principi e i driver di migrazione in Cloud; tali elementi, infatti, sono direttamente influenzati da obiettivi, scelte e iniziative che l'Amministrazione ha deciso di perseguire o che intende realizzare nel medio e lungo termine;
- valutazioni strategie di migrazione: analisi dei gap tra contesto as-is, emerso nella fase di assessment, e vision strategica con conseguente valutazione delle possibili strategie di migrazione dei singoli applicativi e definizione dei singoli path di migrazione in Cloud per ogni applicativo. Inoltre, sulla base delle caratteristiche degli applicativi oggetto di analisi e delle linee guida architetturali presenti all'interno dell'Amministrazione vengono definiti i requisiti per la "landing architecture Cloud" necessari per il corretto indirizzo delle fasi successive di progettazione e realizzazione. Tali attività pongono infatti le basi per la definizione della roadmap e, quindi, delle "wave" di migrazione.

In virtù della finalità di portare le Amministrazioni all'interno dell'infrastruttura PSN per garantire adeguati livelli di sicurezza, la migrazione come anticipato anche nel Progetto di Fattibilità, sarà effettuata, ad eccezione dei casi di Housing, principalmente in modalità Re-Host (Lift&Shift) che consiste nel "prendere" (Lift) l'intero servizio, compreso di infrastruttura, architettura, dati e traffico e "spostarlo" su un hosting cloud (Shift) senza modifiche al core dell'applicativo. La migrazione potrà esser effettuata in due modalità manuale e automatizzata. Questa strategia permette di effettuare un primo passo verso il cloud lasciando aperta la possibilità, successivamente, di implementare ulteriori miglioramenti all'applicativo che consentano di sfruttare ulteriormente i vantaggi del cloud andando ad utilizzare altre strategie di migrazione previste dal paradigma delle 6R, ossia Re-Platform e Re-Architect.

### Step 3.1 | Progettazione e Pianificazione Migrazione – Landing Architecture

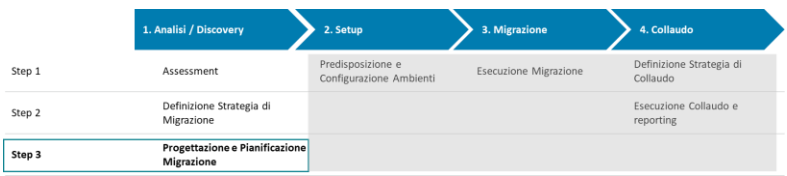



**Figura 41 Step 3 - Progettazione e Pianificazione Migrazione**

In funzione della strategia di migrazione, la progettazione prevede in un approccio incrementale la definizione dei requisiti implementativi e la relativa definizione del piano operativo per la migrazione.

L'approccio metodologico prevede in primo luogo **l'individuazione dei requisiti applicativi da utilizzare come input per la definizione dell'High Level Architecture**. Nello specifico, possono essere identificati, a titolo esemplificativo e non esaustivo, i seguenti requisiti in funzione del modello Cloud target (es. IaaS, PaaS, SaaS):

- compute: tipo di istanze, tipo server (es. Web Server/ Application Server), # VM, # Core per VM, VM
  uptime (%), CPU utilization (%), etc.;
- storage: tipo storage (SAN, NAS, Object, Deep Archive), tipo storage in cloud, RAID level, Capacity (GB), Storage utilization (%), # IOPS requests, backup capacity (GB);
- data Base: tipo istanza/ servizio DBaaS, # istanze DB, target engine type, target DB edition, target license model, target deployment type (es. multiple availability zones), CPU, Memory, Storage;
- network: # load balancer, volumi di traffico, CDN;
- additional services: encryption, key management, firewall, monitoring tool, repository sw, CI/CD tool;
- stack software target;
- previsione di crescita dell'infrastruttura;
- requisiti High Availability/ DR.

### Step 3.2| Progettazione e Pianificazione Migrazione – Definizione Piano di Migrazione

Lo step si compone delle attività necessarie a definire un master plan di tutti gli interventi necessari per realizzare la strategia di migrazione prevista per la specifica Amministrazione; ciascun intervento sarà quindi declinato in un piano operativo e attuativo di dettaglio rolling, in funzione dell'orizzonte temporale previsto per quell'intervento (breve, medio o lungo termine).

Il masterplan ed i relativi piani operativi, prima di poter essere considerate esecutivi, richiederanno un formale **processo di valutazione da parte dell'Amministrazione** in termini di sinergie, effort/budget richiesto, prioritizzazione, sia rispetto alla rilevanza dell'iniziativa in sé che rispetto a esigenze/ vincoli di business.

Per la definizione di una roadmap attuativa che tenga effettivamente in considerazione tutti gli aspetti rilevanti ai fini della definizione delle tempistiche, delle correlazioni e delle sinergie tra le attività, il costituito RTI propone l'adozione di un approccio fortemente iterativo che parte con la condivisione e

approvazione del **Master Plan high level** e successivamente prevede la condivisione e approvazione dei **piani operativi**.

La **roadmap del progetto di migrazione** considera le caratteristiche del parco applicativo e infrastrutturale nonché i vincoli temporali ed i livelli di servizio che devono essere garantiti, fornisce una overview e una stima della durata e della complessità del progetto di migrazione e si articola nelle seguenti macro-attività, proprie di un **progetto di Cloud migration**:

- **Solution detailed design**: design di dettaglio della landing zone target, disegno dei workload e di dettaglio dell'architettura logica e fisica;
- **Scheduling & technical design**: schedulazione di dettaglio del moving delle applicazioni, definizione approccio tecnico di migrazione, setup ambiente e tool di migrazione;
- **Migration execution**: esecuzione delle wave di migrazione, costruite in funzione dei livelli di affinità delle applicazioni e seguendo un livello di criticità crescente, data migration/ replication;
- **Disaster Recovery roll-out:** se previsto roll-out dell'infrastruttura di Disaster Recovery;
- **Performance, UAT & Security Testing:** esecuzione dei test di performance, funzionali, collaudo utente e dei security test**;**
- **Cutover & Go-live**: turn-down finale dell'infrastruttura as is.

### 22.6.2 MAKE - Fase di Setup

Il setup rappresenta la fase propedeutica all'effettiva esecuzione della migrazione ed è finalizzata a garantire un'efficace predisposizione dell'ambiente target su cui dovranno essere movimentati i servizi/applicazioni dell'Amministrazione.

In tale fase saranno quindi svolte le seguenti attività:

- **progettazione operativa e di dettaglio**: tale attività partendo dalla progettazione iniziale di più alto livello, definisce le singole componenti da implementare, gestendo anche le possibili 'eccezioni' che si dovessero riscontrare nella fase make;
- **predisposizione dell'infrastruttura target presso i DC del PSN:** tale attività si traduce nella configurazione degli ambienti target, che dovranno ospitare l'Amministrazione;
- **predisposizione dell'infrastruttura di networking relativa alla connessione tra la PA e i nuovi DC**, qualora tale servizio, aggiuntivo rispetto alla migrazione, sia stato richiesto dall'Amministrazione all'interno del Piano dei Fabbisogni.

### 22.6.3 MAKE - Fase di Migrazione

La migrazione vera e propria si compone di step successivi la cui responsabilità operativa è in carico ai partecipanti al team di progetto in base a quanto definito nel Gantt di progetto.

Le **macro-attività** previste, così come individuato nel Progetto di Fattibilità, possono essere identificate nelle seguenti:

- **trasferimento dei workload**, e conseguente esecuzione di test "a vuoto" dell'ambiente migrato;
- **trasferimento dei dati**, ovvero esecuzione dell'effettivo spostamento dei dati dal Data Center dell'Amministrazione all'interno dell'infrastruttura del PSN;
- **implementazione policy di sicurezza**, ovvero applicazione delle misure di sicurezza definite in sede di progettazione ed in linea con i dati/servizi gestiti dall'Amministrazione; per lo svolgimento di tali attività, in particolare in presenza di dati critici/strategici gestiti dall'Amministrazione, potrà essere richiesto il supporto di figure professionali dedicate (es. Senior Information Security Consultant, Junior Information Security Consultant, etc.) tramite l'attivazione dei Professional Services previsti da Capitolato;
- **impostazione del monitoraggio**, ovvero configurazione dei servizi previsti per il monitoraggio delle infrastruttura/servizi dell'Amministrazione ospitati presso l'infrastruttura del PSN.

L'implementazione può coinvolgere, in funzione della tipologia di servizio da migrare, le strutture deputate all'esercizio dell'infrastruttura del PSN, a cui sono demandate attività di installazione/configurazione infrastrutturale, in virtù delle specifiche tecniche definite da parte del team di progetto.

L'onboarding dei servizi di un'Amministrazione deve prevedere oltre ad un approccio metodologico strutturato alle attività esecutive della migrazione, anche **l'adozione di specifiche soluzioni tecnologiche** al fine di favorire un controllo ed una razionalizzazione degli interventi**.**

In tal senso il costituito RTI, sulla base delle proprie Best Practice adotterà **l'uso di strumenti e tecnologie allo stato dell'arte** per favorire in tempi, modi e sicurezza, l'operazione di migrazione.

I Tool in uso al costituito un efficace fase permetteranno diverse tipologie di migrazione sulla base delle tecnologie che adottano i sistemi all'Amministrazione. Chiaramente più la maturità 'tecnologica' dell'Amministrazione sarà alta (con elevata disponibilità di ambienti virtualizzati), più il metodo adottato assicurerà, minor impatto sui tempi di fermo dei servizi (sino alla possibilità di migrare con i servizi tutti live), tempi migliori e sicurezza nello spostamento dei servizi con possibilità di rollback e con minimi impatti, in caso di problemi. Ogni tipologia farà riferimento ad una matrice di compatibilità relativa alla

configurazione della singola VM che deve essere migrata. A titolo esemplificativo si rappresentano alcune modalità di migrazione possibili:

- **Bulk Migration** (La VM si sposta con un fermo della durata di un reboot):
  - la replica avvia un processo sincronizzato di trasferimento completo delle VM sul sito di destinazione. Il tempo necessario per la replica dei dati dipende dalle dimensioni delle VM e dalla larghezza di banda disponibile;
  - la larghezza di banda viene consumata dal processo di replica a seconda di come il carico di lavoro modifica i blocchi su disco;
  - al termine della sincronizzazione FULL dei dati viene fatto partire un processo di sincronizzazione del DELTA fino all'apertura della finestra prestabilita di migrazione quando sarà possibile effettuare lo switchover delle VM. Utilizzando l'opzione di migrazione pianificata, lo switchover può avvenire durante una finestra di manutenzione prestabilita;
  - dopo lo switchover la VM di origine viene spenta e la VM di replica migrata viene accesa sul sito di Landing. Se per qualche motivo una VM non riesce ad accendersi sul sito di Landing, la nuova VM verrà spenta (oppure rimarrà spenta) e l'originale verrà riaccesa. (in questo caso rimane una copia della VM sul sito origine);
  - le VM originali verranno rinominate utilizzando un suffisso per evitare un conflitto di denominazione con le VM migrate;
- **Live Migration** (La VM si sposta senza fermare il servizio):
  - è possibile migrare un grande numero di VM in tempo reale (fino a 200VM per volta);
  - si può migrare anche una singola VM per volta;
  - è possibile impostare una finestra di manutenzione per l'attività di switchover;
  - una volta individuato un gruppo di VM per la migrazione, RAV esegue la sincronizzazione iniziale e continua a replicare il delta delle modifiche fino a quando non viene raggiunta la finestra di switchover;
  - è possibile migrare contemporaneamente più VM, quando la fase di replica raggiunge la finestra di manutenzione stabilita viene avviata la procedura di migrazione. Lo switchover live avviene in modo seriale;
  - la VM viene rimossa dal cluster di Landing e migrata sul cluster di destinazione. Non rimane una copia sul cluster origine;
- **Cold Migration:**

- è selezionata in automatico quando le VM da migrare sono spente.

Le VM che vengono migrate da un sito all'altro possono essere comunque riportate indietro con lo stesso strumento, nel caso si voglia mantenere la possibilità di un ripristino della VM originale è sempre consigliato procedere ad un backup delle VM sul sito di partenza a carico del cliente.

Questi tool consentono, di migrare VM basate su tecnologie di virtualizzazione diverse ed anche di cambiare la tipologia, in alcuni casi, della vm di atterraggio, ove l'Amministrazione volesse cambiare l'ambiente operativo di virtualizzazione, anche se chiaramente, potranno cambiare le modalità con cui la migrazione avviene.

Ogni prodotto ha una sua matrice di compatibilità per poter funzionare al meglio, ma chiaramente ci si potrà basare su tools di migrazione meno evoluti e fondati su operazioni di backup e restore, che sebbene senza le potenzialità di quanto rappresentato, automatizzano in ogni caso il processo, favorendo la sicurezza di un'operazione che deve assicurare: il minimo possibile di fermi dei servizi (Se non l'assenza completa), la possibilità di tornare alla configurazione di partenza in caso di problemi inattesi, la garanzia di dati e configurazioni degli ambienti dell'Amministrazione.

### 22.6.4 GO - Fase di Collaudo

L'ultima fase del processo di migrazione prevede l'esecuzione dei test di accettazione finalizzati a garantire che tutti i dati che si vuole trasferire sono stati effettivamente migrati correttamente. A seguito del collaudo funzionale della intera infrastruttura di ogni PA, il costituito RTI prevederà l'attivazione di tutti i Servizi richiesti dalla PA (cfr. documento "Specificazione delle caratteristiche del servizio e della gestione").

Per garantire un'efficace fase di test di accettazione, il costituito RTI prevede di eseguire le seguenti attività:

- predisposizione e condivisione con l'Amministrazione di un **documento di Strategia di Collaudo**, contenente il dettaglio del perimetro dei test da eseguire sui servizi della PA oggetto di migrazione, test list, livello di copertura, script di test, exit criteria, etc.;
- gestione della **Cabina di Regia delle sessioni di test**, al fine di coordinare il coinvolgimento del personale dell'Amministrazione, con particolare riferimento allo svolgimento di eventuali test di verifica su applicativi critici per il business della stessa;
- predisposizione della **reportistica di avanzamento dei test** con relativa evidenza dei principali KPI (test eseguiti, test OK, test KO, attuali incidenti/anomalie aperte, etc.); tale reportistica sarà messa a disposizione dell'Amministrazione sul Portale della Fornitura.

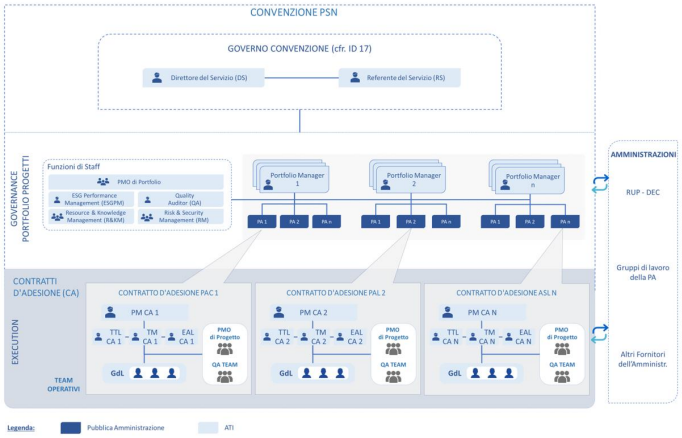
Per il Collaudo, il costituito RTI prevede di eseguire, anche in linea con il Manuale di Abilitazione al Cloud redatto da AgID, le seguenti tipologie di test:

- **test di completezza:** test finalizzati a verificare che tutti gli oggetti rilevanti a livello business oggetto di migrazione siano stati effettivamente migrati con successo, in tale ambito quindi ricadono le verifiche relative a:
    - **verifiche di riconciliazione** per valutare la completezza del patrimonio informativo migrato, ovvero assicurare che il numero di entità nel sistema sorgente sia il medesimo nel sistema di destinazione;
    - **verifiche di validazione orizzontale** per assicurare, tramite un conteggio dei valori rilevanti delle entità le trasformazioni, gli arricchimenti di dati, i consolidamenti e le esclusioni non abbiano alterato aspetti fondamentali delle unità di migrazione;
- **appearance test**: test che mirano a ridurre il rischio di inconsistenza dei dati; in questi tipi di test, il costituito RTI coadiuvata da personale dell'Amministrazione, esperta di dominio, confrontano manualmente i dati presenti nel sistema sorgente e destinazione attraverso l'interfaccia utente dell'applicativo;
- **test di integrazione:** test finalizzati a verificare la corretta comunicazione tra applicazioni/servizi che prevedono scambi e flussi dati;
- **test di sicurezza:** test aggiuntivi proposti dal costituito RTI, in presenza di dati critici/strategici in uso presso l'Amministrazione, al fine di verificare l'applicazione delle adeguate misure di sicurezza presso l'infrastruttura del PSN; per l'esecuzione di tali test (es. Penetration Test, etc.) sarà prevista l'attivazione dei Professional Services previsti da Capitolato al fine di integrare il team mix della migrazione con specifiche figure professionali, esperte di sicurezza (es. Senior Penetration Tester, Junior Penetration Tester, Security Solution Architect, etc.). È comunque previsto un livello standard di test di sicurezza, per il collaudo attraverso l'esecuzione di Vulnerability Assessment automatici, per certificare la sicurezza dell'infrastruttura PSN.

# 23 ID 21 – Valutativo - Miglioramenti del modello organizzativo, delle metodologie e degli strumenti che il concorrente si impegna ad adottare per il monitoraggio e il controllo della migrazione al fine del rispetto delle tempistiche previste

## 23.1 Executive Summary

Il costituito RTI, in relazione alla premialità connessa al miglioramento delle modalità per la migrazione al Cloud in termini di monitoraggio e gestione della migrazione, propone un **framework organizzativo e metodologico pienamente integrato** con **la governance complessiva della Convenzione** (cfr. ID 17) e con le modalità operative previste per l'esecuzione delle fasi operative (cfr. ID 20).




Come già visto nel capitolo 19, il **modello organizzativo del servizio di migrazione** prevede **un layer operativo di execution**, in cui convergono i team dedicati ai singoli contratti di adesione ed **un layer di governo del portfolio dei progetti di migrazione**, dedicato alla governance trasversale che attinge dalle funzioni di Staff previste dalla Governance complessiva della Convenzione e finalizzato alla gestione dei processi di qualità, PMO, monitoraggio performance, etc.

La **componente trasversale** garantisce inoltre la possibilità di diffondere sui vari team operativi le best practice e le lesson learned acquisite nel corso dei progetti, nonché di effettuare un processo più efficace ed efficiente di staffing delle risorse, avendo piena visibilità sulle diverse fasi progettuali in essere e prospettiche.

Ai fini di migliorare l'approccio metodologico per il monitoraggio e la gestione della migrazione, **il costituito RTI introduce 6 metodologie dedicate presenti nel framework EMG2C** e di seguito rappresentate che sono a

| Metodologia | Pre-Avvio del Progetto di Migrazione | Progetto Migrazione in Corso | | | |
|---|---|---|---|---|---|
| | | Analisi/ Discovery | Setup | Migrazione | Collaudo |
| Gestione del Portfolio | ✔ | ✔ | ✔ | ✔ | ✔ |
| Monitoraggio e Controllo del Progetto | | ✔ | ✔ | ✔ | ✔ |
| Monitoraggio Performance del Progetto | | ✔ | ✔ | ✔ | ✔ |
| Gestione dei Rischi | | ✔ | ✔ | ✔ | ✔ |
| Change Management e Formazione | | | | | ✔ |
| Gestione della flessibilità organizzativa | ✔ | ✔ | ✔ | ✔ | ✔ |

supporto di tutte le fasi (Analisi/Discovery, Setup, Migrazione e Collaudo).

Infine, il framework contiene un set di **strumenti per il monitoraggio e gestione della migrazione** già utilizzati in contesti analoghi dalle società del costituito RTI (es. Planner Risorse, Issue Log, KPI Monitoring Dashboard), e perfettamente funzionali alle metodologie previste.

Per rispondere al criterio ID 21, nel documento sarà illustrato inizialmente **il modello organizzativo** proposto per il monitoraggio e la gestione della migrazione (cfr. paragrafo 23.2), successivamente **le metodologie a supporto** identificate (cfr. paragrafo 23.3) ed infine **gli strumenti messi a disposizione** (cfr. paragrafo 23.4).

## 23.2 Modello Organizzativo

### 23.2.1 Modello Organizzativo per la gestione delle attività di governance e delle attività operative

In questo paragrafo è illustrato il modello organizzativo per la migrazione dei servizi delle Pubbliche Amministrazioni nel PSN, con l'obiettivo di migliorare il monitoraggio e il controllo delle attività necessarie a tale scopo. Come già descritto nel Capitolo ID 17, il costituito RTI propone un modello organizzativo basato su layer multipli (Governo Convenzione, Governance Portfolio Progetti, Execution), illustrato nella Figura 42. Nel paragrafo successivo vengono descritti i diversi ruoli presentati, con il dettaglio dei compiti e delle responsabilità, con un modello organizzativo basato su layer multipli. Nel paragrafo successivo vengono descritti i diversi ruoli presentati, con il dettaglio dei compiti e delle responsabilità.

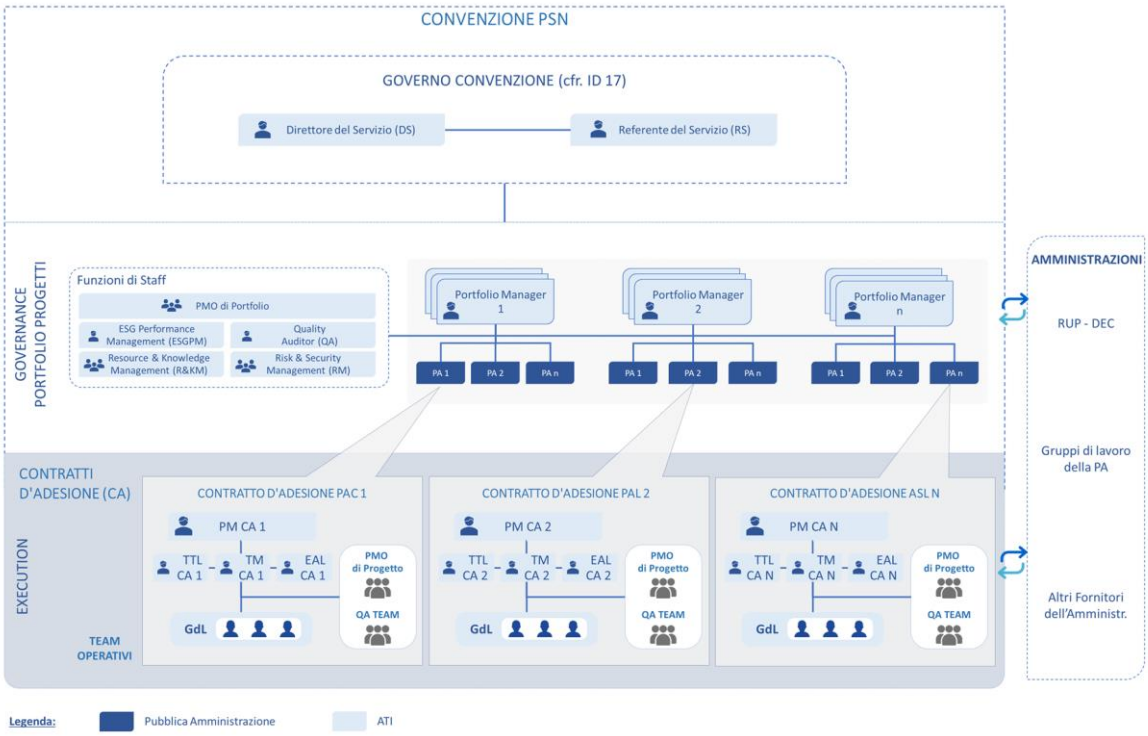



**Figura 42 Modello organizzativo per la gestione delle attività di migrazione**

### 23.2.2 Dettaglio ruoli del modello organizzativo

Nel seguito, sono dettagliati i ruoli presentati nel modello organizzativo, fornendo una panoramica complessiva di responsabilità ed attività di ciascun ruolo all'interno delle attività di migrazione.

*Tabella 9 Dettaglio dei ruoli del modello organizzativo*

| **Governo Convenzione** | |
|---|---|
| **Ruolo** | **Descrizione** |
| Direttore del Servizio | Tali figure vengono riportate nel presente paragrafo in quanto coinvolte nel processo di monitoraggio e gestione dei servizi di Migrazione. Per la descrizione di dettaglio delle figure rappresentate nel layer in oggetto si rimanda al Capitolo ID 17. |
| Referente del Servizio | |
| **Layer Governance Portfolio Progetti** | |
| **Ruolo** | **Descrizione** |

| | |
|---|---|
| Portfolio Manager | Nel perimetro delle figure di Staff previste nell'Organizzazione complessiva descritta nel Capitolo 19, sono riportate quelle direttamente coinvolte nel processo di monitoraggio e gestione dei servizi di Migrazione. Per la descrizione di dettaglio delle figure rappresentate nel layer in oggetto si rimanda al Capitolo 19. |
| PMO di Portfolio | |
| ESG Performance Management | |
| Quality Auditor | |
| Resource & Knowledge Management | |
| Risk Management | |

| **Layer Operativo** | |
|---|---|
| **Ruolo** | **Descrizione** |
| PMCA | Il **PMCA costituisce l'interfaccia unica verso l'Amministrazione Aderente**, in particolare verso il RUP e verso il DEC dell'Amministrazione, per tutti gli aspetti riguardanti l'**esecuzione del Contratto e** per tutti i **servizi contrattualizzati**.<br>In particolare, le **principali responsabilità** in capo a questa figura professionale sono:<br>• Fornitura di una **vista integrata dell'andamento** dell'intera fornitura, garantendo gli adempimenti previsti in linea con le tempistiche concordate;<br>• **Coordinamento ed escalation** nella definizione di **soluzioni** e nella gestione di eventuali **problematiche/criticità** interne al singolo CA;<br>• **Coordinamento**, con il supporto del TTL, all'**erogazione dei servizi** sulla base di quanto previsto e contrattualizzato nel CA;<br>• Fornitura all'Amministrazione di **reportistica periodica** relativa agli asset gestiti, ticket elaborati nel periodo di riferimento, livelli di servizio conseguiti con l'eventuale calcolo delle penali applicabili, rendicontazione, **stati di avanzamento** (SAL) delle attività remunerate a corpo;<br>• **Organizzazione e pianificazione** delle attività inerenti alla **rilevazione della soddisfazione degli utenti**. |

| | |
|---|---|
| Technical Team Leader | Figura dedicata che seguirà tutte le fasi più strettamente legate agli **aspetti operativi** e supervisionerà il gruppo di lavoro dal **punto di vista tecnico**. In particolare, si concentrerà sull'**analisi della domanda** e sulla creazione di obiettivi per il Gruppo di lavoro sull'**identificazione anche preventiva di issue e criticità**, gestendo gli aspetti di **sicurezza** ed eventuali **change request**, garantendo l'allineamento e la produttività del team operativo. |
| Transition Manager | Esperto di **best practice** ITIL di **Service Transition**, pianifica e conduce, implementando le linee guida stabilite dal EAL, il progetto di presa in carico dei servizi da parte della struttura operativa del costituito RTI. Ingaggia le strutture operative per le attività necessarie alla transizione post migrazione, **concorda con i Responsabili dell'Amministrazione** le **tempistiche** e ne traccia l'avanzamento. **Riferisce al PMCA** sullo stato delle attività e si interfaccia direttamente con le funzioni tecniche dell'Amministrazione nelle sessioni di pianificazione e di stato avanzamento lavori. |
| Enterprise Architect Lead | **Punto unico** di ingresso per le **richieste di supporto specialistico**, si configura come il riferimento del layer operativo in **ambito metodologie**, sia per il costituito RTI sia per l'Amministrazione, per i processi di Service Management, Project e Risk Management ed Enterprise Architecture. È inoltre il **focal point** del costituito RTI per l'identificazione e la standardizzazione di **casi di successo** da riproporre, in **ottica di riusabilità**, nell'ambito della convenzione. |
| Gruppo di Lavoro | Team dedicato al singolo CA che ha in carico le **attività operative demandate dal TTL** e necessarie per il completamento del progetto di Migrazione.<br>Il Gruppo di Lavoro **è composto dalle figure tecniche professionali** in rispetto di quanto offerto del costituito RTI nel **Progetto di Fattibilità**. |
| PMO di Progetto | **Supporta le attività progettuali** in termini di presidio dei servizi di PMO, nella **pianificazione e nel monitoraggio delle attività,** tenendo conto delle interdipendenze tra le diverse iniziative attivate all'interno del singolo CA. **Verifica e valida la produzione di deliverable** di livello **operativo** e di **reportistica**, fornendo spunti e contributi per la produzione di report executive. Raccoglie e sistematizza le pratiche adottate durante la gestione operativa, valorizzando **lessons learned** e **best practice**. Vigila sul **corretto uso degli strumenti progettuali** e sul rispetto delle cerimonie di comunicazione verso il |

| | |
|---|---|
| | cliente. Governa ed agisce nei confronti di eventuali rischi operativi ed issue progettuali, ottimizzando l'impiego delle risorse. Tra le ulteriori attività in carico abbiamo:<br>• Formalizzazione e aggiornamento dei **Piani di Lavoro;**<br>• **Monitoraggio dello stato di avanzamento** dei progetti mediante predisposizione di documenti quali Dashboard direzionali, SAL;<br>• **Coinvolgimento delle strutture interessate** sia negli incontri sia nella produzione di documentazione ufficiale connessa alle attività progettuali. |
| Quality Assurance Team | Tale struttura è deputata a garantire che il **risultato delle attività di migrazione soddisfi i requisiti qualitativi stabiliti** ex ante, nonché le richieste e le aspettative dell'Amministrazione coinvolta. Tale compito attiene a diversi domini, dal **monitoraggio dei processi e degli SLA**, al **controllo sui dati** e sulla qualità degli stessi, alla **verifica del corretto aggiornamento della documentazione** progettuale. Dispone, quando necessario, **azioni correttive** di rilavorazione, nonché **azioni preventive** al sorgere di particolari criticità sul piano operativo. |

### 23.2.3 Protocolli di Comunicazione

Si dettagliano nel seguito, per il layer operativo, i principali protocolli e metodi di comunicazione che il costituito RTI intende adottare per assicurare una corretta e tempestiva gestione delle attività di migrazione. Per tutti i protocolli, comitati e checkpoint, che fanno riferimento ai layer di Governo di Convezione e Governance Portfolio Progetti è possibile consultare il capitolo ID 17.

*Tabella 10 Dettaglio dei protocolli di comunicazione*

| **Protocolli di Comunicazione** | | | | |
|---|---|---|---|---|
| Nome | Descrizione | Esterno/ Interno | Attori coinvolti | Frequenza |
| Kick-off di Progetto | Incontro di **condivisione del piano di lavoro** del programma/progetto in termini di **contenuti**, | Interno | PMCA<br>Technical Team Leader | - |

| | | | | |
|---|---|---|---|---|
| | obiettivi, macro-fasi, interventi, **tempi e deliverable**. | | PMO di Progetto<br>Quality Assurance Team<br>Referenti Amministrazione<br>Stakeholder esterni | |
| SAL di Execution | Incontri di **rendicontazione dell'avanzamento delle attività operative**, dove vengono evidenziate attività e milestones inerenti alle diverse fasi progettuali. Tali meeting, calendarizzati con **cadenza almeno quindicinale**, hanno **carattere operativo** e coinvolgono principalmente il **layer di execution** nelle figure del Project Manager, del Technical Lead, il PMO di progetto e la funzione di QA, insieme ai referenti dell'Amministrazione ed agli eventuali stakeholder esterni coinvolti nel processo di migrazione. | Interno | PMCA<br>Technical Team Leader<br>PMO di Progetto<br>Quality Assurance Team<br>Referenti Amministrazione<br>Stakeholder esterni | Bisettimanale |
| Review chiusura Progetto | Incontro di condivisione delle **attività concluse** e dei deliverable prodotti; verifica degli **SLA**; validazione dei risultati, eventuale chiusura del programma/progetto.<br>Durante il meeting vengono inoltre individuate e clusterizzate le principali **best practice** che possono essere potenzialmente **riutilizzate** in ottica di **efficientamento del governo** della Convenzione in ambito **migrazione**. | Interno | PMCA<br>Technical Team Leader<br>PMO di Progetto<br>Quality Assurance Team<br>Referenti Amministrazione<br>Stakeholder esterni | - |

Per la descrizione dei momenti di comunicazione in riferimento alle varie fasi progettuali, sia operative che strategiche, è possibile fare riferimento al paragrafo “Processi / Interazioni con il Concedente e con i Fornitori Terzi” del ID 17.

## 23.3 Metodologie

Per la fornitura in oggetto, il costituito RTI propone un set di metodologie in grado di coprire le diverse necessità di monitoraggio e controllo delle attività di migrazione, basate sui seguenti principi cardine:

- l’adozione di una **metodologia integrata** nel framework di migrazione **EMG2C** (**Explore, Make, Go to Cloud**) in grado di accompagnare l’Amministrazione in tutto il ciclo di vita del progetto di migrazione, dalla declinazione delle esigenze strategiche e gestione operativa, alla governance dei progetti fino alla rilevazione degli obiettivi raggiunti, coniugando le best practice di gestione dei progetti e dei servizi digitali (PMI-PMP, Prince2, ITIL) con le logiche innovative derivanti dall’approccio iterativo del framework Agile SCRUM;
- la predisposizione di **strumenti e soluzioni di governance** in grado di offrire alle Amministrazioni sia gli indicatori convenzionali circa il governo e il controllo della Fornitura sia gli strumenti per ottenere una visione organica delle progettualità in corso e del relativo stato di avanzamento rispetto agli obiettivi;
- la definizione di **meccanismi di check dei risultati raggiunti**, al fine di verificare la coerenza delle soluzioni realizzate rispetto alle attese, gli scostamenti tra risorse pianificate e effettivamente impiegate e le eventuali lesson learned e best practice da applicare su altri progetti, anche al fine di creare modelli comparativi da utilizzare su altri Contratti d’adesione.

In virtù dei servizi previsti per le attività di Monitoraggio e Controllo della Migrazione, dell’organizzazione delle attività, degli stakeholder coinvolti e dei risultati attesi, l’approccio proposto dal costituito RTI risponde a **chiari razionali** di:

- iteratività dei processi di PM;
- impiego di tecniche e strumenti per la misurazione degli impatti, ex-ante ed ex-post;
- interazioni frequenti con l’Amministrazione e con gli stakeholder;
- standardizzazione dei risultati in ottica di creazione di asset riutilizzabili;
- spinta alla creazione e diffusione di know-how.

Di seguito si offre una vista sinottica delle metodologie impiegate, con dettaglio per le diverse fasi di un’iniziativa di migrazione:

| Metodologia | Pre-Avvio del Progetto di Migrazione | Progetto Migrazione in Corso | | | |
|---|---|---|---|---|---|
| | | Analisi/ Discovery | Setup | Migrazione | Collaudo |
| Gestione del Portfolio | ✓ | ✓ | ✓ | ✓ | ✓ |
| Monitoraggio e Controllo del Progetto | | ✓ | ✓ | ✓ | ✓ |
| Monitoraggio Performance del Progetto | | ✓ | ✓ | ✓ | ✓ |
| Gestione dei Rischi | | ✓ | ✓ | ✓ | ✓ |
| Change Management e Formazione | | | | | ✓ |
| Gestione della flessibilità organizzativa | ✓ | ✓ | ✓ | ✓ | ✓ |

**Figura 43 Metodologia adottata per le diverse fasi**

### 23.3.1 Gestione del Portfolio

Considerata la dimensione della Fornitura in termini di progetti, impatti sui sistemi IT ed attori coinvolti, si ritiene necessaria una metodologia per la gestione integrata delle singole iniziative, evidenziandone le interrelazioni (ove presenti) e gli impatti, anche con piani esterni al contesto della Fornitura. La metodologia adottata garantisce un presidio capillare di tutte le iniziative di migrazione a Livello Portfolio Progetti: la pianificazione integrata per questo livello armonizza e combina i diversi Contratti d'adesione in capo a ciascuna delle diverse Amministrazioni, tenendo in considerazione eventuali interdipendenze, valorizzando le sinergie e la corretta gestione dei rischi.

Il processo complessivo di gestione del portafoglio progetti si compone di 3 fasi principali, quali:

- **definizione**: in questa prima fase si prevedono attività iterative mirate alla formulazione dei benefici attesi, allo sviluppo del programma nei diversi progetti e del disegno tecnico di alto livello, andando a costruire il Master Plan delle iniziative;
- **erogazione**: attraverso un processo ciclico, viene definito e aggiornato il Master Plan delle iniziative e vengono eseguite attività di monitoraggio continuo degli indicatori di performance a livello di portfolio;
- **chiusura**: tale fase consiste nell'identificazione di eventuali gap emersi rispetto agli obiettivi attesi, nella verifica dei benefici prodotti e dell'effettivo completamento delle attività di migrazione.

### 23.3.2 Monitoraggio e Controllo del Progetto

La metodologia di monitoraggio del Progetto ha l'obiettivo di supportare le Amministrazioni nella corretta gestione delle iniziative, in particolare nell'uso delle risorse (tempi, costi, personale) e nella gestione delle criticità. Gli obiettivi sono di seguito dettagliati:

- **controllare le iniziative nella fase di migrazione,** in termini di rispetto delle tempistiche, dei costi e delle risorse preventivate, dei livelli di qualità erogati dai Fornitori coinvolti e delle performance attese dall'iniziativa;
- **supportare la gestione delle criticità** eventualmente emerse nella fase realizzativa con l'individuazione di opportune azioni correttive;
- **attivare un processo di miglioramento continuo**, attraverso un meccanismo di verifica delle previsioni di costo, delle stime del consumo di risorse e delle quantificazioni dei risultati/benefici attesi.

Il costituito RTI prevede la verifica dell'avanzamento dei piani di realizzazione delle iniziative in modalità continuativa, secondo un approccio a tre fasi, agendo su tutte le variabili di controllo e producendo:

1. **una valutazione dello stato di avanzamento di ogni singola iniziativa,** effettuato secondo un processo bottom-up dal Team di Progetto, per poi abilitare un processo di controllo top-down secondo due tipologie di check:
    - **controllo stato avanzamento delle tempistiche:** confrontando lo stato delle attività a consuntivo rispetto allo stato previsto per le medesime attività, viene individuata la percentuale delle azioni in ritardo;
    - **controllo consumo risorse:** viene verificato se il consumo risorse è allineato al piano previsto e quantificato l'eventuale scostamento. L'entità percentuale ed il valore assoluto dello scostamento evidenziano il livello di criticità dell'iniziativa;
2. **una sintesi direzionale dello stato avanzamento ed individuazione delle attività critiche**, condotta attraverso l'analisi del portfolio progetti ed il posizionamento in una matrice sui cui assi vengono misurati l'entità dell'eventuale ritardo ed il livello di efficienza individuato;

3. **una definizione dei piani di recupero, che prevede** l'elaborazione di azioni correttive per le iniziative critiche, con il coinvolgimento dei responsabili delle iniziative dell'Amministrazione e dei Project Manager. Questi ultimi formulano i piani di recupero volti a colmare gli scostamenti evidenziati nel controllo stato avanzamento delle tempistiche e nel controllo consumo risorse.

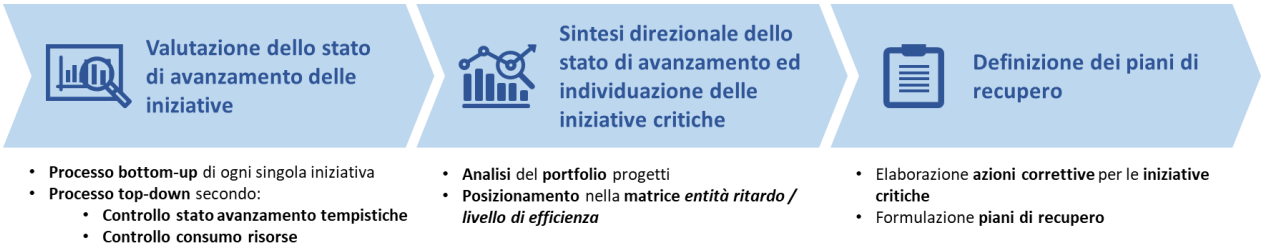



**Figura 44 Processo di verifica dell'avanzamento progettuale**

### 23.3.3 Monitoraggio delle Performance del Progetto

I KPI associati alle attività di migrazione vengono controllati secondo un **processo di monitoraggio strutturato,** che fa leva su un set di KPI standard condiviso per l'intera fornitura. L'individuazione degli indicatori di performance e la prima misurazione avvengono nelle fasi precedenti all'avvio dell'iniziativa di migrazione. Per l'identificazione degli indicatori, l'approccio proposto è **focalizzato su seguenti punti principali**:

- utilizzo dei dati di cui dispone il costituito RTI, legati a precedenti esperienze progettuali, per stimare i valori degli indicatori di performance. Laddove l'Amministrazione non abbia dati, il costituito RTI andrà ad utilizzare valori di confronto e valori "proxy" stimati (es. incidenza dei costi strutturali sui costi hardware);
- supporto all'Amministrazione nel selezionare gli indicatori generali più idonei (ove possibile e/o necessario);
- proposizione di ulteriori indicatori basati su:
    - quanto previsto da linee guida e best practice di riferimento, non solo in termini di gestione dei progetti ma in particolare per la realizzazione dei progetti di migrazione;
    - esperienze di successo del costituito RTI in progetti assimilabili;
    - best practice di mercato per **cluster tematici/tecnologici di riferimento.**

Gli indicatori aggiuntivi verranno sottoposti ai referenti dell'Amministrazione e, se approvati, inseriti nel monitoraggio durante le fasi di erogazione dei servizi ed aggiunti alla reportistica predisposta.

Si presenta di seguito un elenco, esemplificativo e non esaustivo, delle misure interne che il costituito RTI intende implementare per migliorare il Monitoraggio della performance di Progetto. I valori target per ciascun indicatore saranno stabiliti dal costituito RTI di concerto con le Amministrazioni.

*Tabella 11 Esempi di KPI per monitoraggio della performance di progetto*

| KPI | Parametro | Elemento valutativo | Unità di misura | Dati da rilevare | Formula |
|---|---|---|---|---|---|
| **Milestone On Time (MOT)** | Tempestività | Il rispetto di milestone progettuali in termini di completamento tempestivo dei vari step di migrazione | Percentuale | Numero di milestone completate in tempo (Nmilestone on time) rispetto al numero di milestone totali (Nmilestone tot) | MOT = (Nmilestone on time)/ (Nmilestone tot) |
| **Average Delay of Milestone (ADM)** | Tempestività | Ritardo medio delle milestone | Giorni lavorativi | Numero di giorni complessivi di ritardo accumulato sul totale delle milestone (Ngiorni rit mil) rispetto al numero totale di milestone (Nmilestone tot) | ADM = (Ngiorni rit mil) / (Nmilestone tot) |
| **Delivery On Time (DOT)** | Tempestività | Rispetto delle tempistiche per la consegna dei deliverable | Percentuale | Numero delle deliverable consegnate nei tempi attesi (Ndeliv on time) rispetto al numero delle deliverable da consegnare (Ndeliv tot) | DOT = (Ndeliv on time)/ (Ndeliv tot) |

| | | | | | |
|---|---|---|---|---|---|
| **Average Delay of Deliverable (ADD)** | Tempestività | Ritardo medio dei deliverable | Giorni lavorativi | Numero di giorni complessivi di ritardo accumulato sul totale delle deliverable (Ngiorni rit deliv) rispetto al numero totale delle deliverable (Ndeliv tot) | ADM = (Ngiorni rit deliv)/ (Ndeliv tot) |
| **Numero di Mancate Approvazioni (NMA)** | Efficacia | Il rispetto di milestone progettuali in termini di numero di mancate approvazioni | Numero Approvazioni | Numero di mancate approvazioni (Nmancate app) | NMA = Nmancate app |
| **Rilievi sull'Iniziativa (RLI)** | Efficacia | Numero rilievi formali emessi nel corso della migrazione | Numero Rilievi | Numero di Rilievi emessi nel corso dell'iniziativa (Nrilevi Iniziativa) | RLI = Nrilevi Iniziativa |
| **Numero di Ripianificazioni (NR)** | Efficacia | Piena rispondenza ai requisiti richiesti in termini di completezza, esaustività, efficacia e chiarezza | Numero Ripianificazioni | Numero ripianificazioni con impatto sul budget e sul calendario deliverable ma con mantenimento della data di fine progetto (Nripianificazioni) | NR = Nripianificazioni |

| | | | | | |
|---|---|---|---|---|---|
| **Non Approvazione Documentazione di Progetto (NADP)** | Qualità | Piena rispondenza ai requisiti richiesti in termini di completezza, esaustività, efficacia e chiarezza | Numero documenti non approvati | Deliverable previsti nella procedura di coordinamento (es. TDM, analisi funzionali, requisiti utente, etc.) non approvati (num doc not appr) | NAPS = num doc not appr |
| **Difettosità Deliverable Rilasciati (DDR)** | Qualità | Piena rispondenza ai requisiti richiesti in termini di completezza, esaustività, efficacia e chiarezza | Numero di riemissioni di deliverable per difetti riscontrati | Deliverable previsti nella procedura di coordinamento (TDM, analisi funzionali, etc.) oggetto di verifica e approvazione da parte dell'amministrazione (num doc ril) | DDR = num doc ril |

### 23.3.4 Gestione dei rischi

Per la metodologia riguardante la gestione dei rischi, si rimanda all'ID22, dove viene illustrata nel dettaglio in risposta allo specifico quesito.

### 23.3.5 Change Management e Formazione

La metodologia proposta per la gestione del change e della formazione rappresenta un elemento fondamentale all'interno della fornitura in quanto contribuisce a plasmare l'organizzazione e i processi dell'Amministrazione in funzione del nuovo paradigma Cloud. **Le attività e metodologie di Change Management** proposte dal costituito RTI per la fornitura sono basate su **standard** riconosciuti a livello internazionale (quali linee guida del **PMI** e del **Change Management Institute**), e garantiranno un'efficace transizione verso il nuovo modello organizzativo, operativo e processuale. Rappresentano un valore aggiunto sia l'esperienza acquisita dal costituito RTI nel riconoscere gli impatti dell'adozione del Cloud, sia l'applicazione **delle relative attività di Change Management fin dalle prime fasi del**

**progetto**, **garantendo** la **coerenza del cambiamento con le linee strategiche**, i programmi operativi, ed il budget dell'Amministrazione. In questo modo il **cambiamento è graduale e il trasferimento delle informazioni è completo e rapido**.

L'approccio proposto è organizzato secondo tre direttive, illustrate di seguito:

- **organizzazione**: valutazione della coerenza del cambiamento con le linee strategiche dell'Amministrazione in funzione della strategia di migrazione adottata; progettazione e pianificazione degli interventi necessari per l'attuazione dei cambiamenti procedurali e/o organizzativi (se presenti); analisi degli impatti sui processi e sull'organizzazione; valutazione di impatti e rischi connessi con il cambiamento;

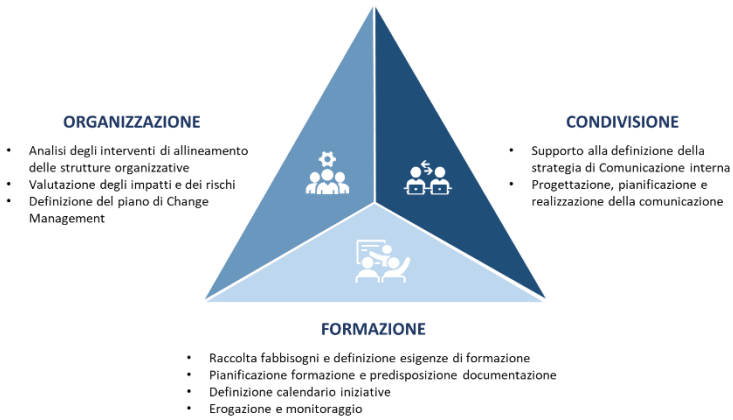



**Figura 45 Approccio per il Change Management e la formazione**

- **condivisione**: supporto alla definizione della strategia di condivisione del cambiamento con le strutture dell'Amministrazione, con l'obiettivo di sviluppare consapevolezza e committment;
- **formazione**: istruzione dei dipendenti in merito al nuovo modus operandi, al funzionamento dell'Amministrazione e alle nuove linee di attività previste dall'evoluzione tecnologica e normativa. In particolare: interpretazione dei fabbisogni di formazione emersi in fase di assessment; pianificazione della formazione e predisposizione della documentazione di supporto; definizione del calendario delle iniziative formative.

### 23.3.6 Gestione della flessibilità organizzativa

In un contesto in forte cambiamento, caratterizzato da continue evoluzioni normative e tecnologiche, il costituito RTI propone, sin dalla fase di avvio della Fornitura, **un approccio organizzativo e operativo basato sulla capacità di reagire con rapidità ed efficacia al presentarsi di situazioni critiche e di instabilità finalizzato al costante rispetto dei livelli di qualità dei servizi erogati**. Le modalità proposte sono funzionali, in un arco di fornitura molto esteso come quello oggetto della fornitura, a fronteggiare eventi "critici", non sempre prevedibili in tempi congrui.

Tali eventi possono essere determinati da:

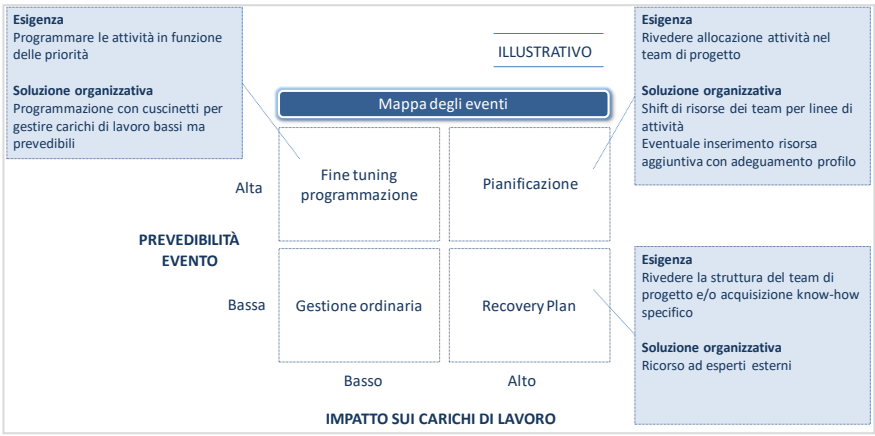
- **fattori endogeni,** ossia **variazioni interne** al contesto della fornitura di **natura organizzativa** quali ad esempio richieste di modifiche/integrazioni di risorse, il *turnover* del personale, etc.; **tecnologica** come ad es. le evoluzioni future previste per le tecnologie Cloud, l'attivazione di nuove piattaforme, etc.; **strategica** come l'integrazione di diverse piattaforme, la spinta all'utilizzo degli open data, etc.;
- **variazioni di Pianificazioni** condivise con l'Amministrazione, derivanti ad es. dalla necessità di attivazione di nuove iniziative progettuali connesse alla fornitura, dall'insorgenza di contingenze, o dal riorientamento delle priorità operative.

L'approccio metodologico proposto dal costituito RTI prevede il **Pillar delle Soluzioni per la flessibilità e tempestività nell'allocazione risorse**, composto da un processo strutturato di gestione e controllo delle criticità, che si articola su 5 fasi, come schematizzato di seguito, atto ad identificare le situazioni critiche, analizzare prontamente gli opportuni cambiamenti, attivare le risposte organizzative ed operative più adeguate, valutare gli effettivi risultati derivanti dall'applicazione delle soluzioni proposte in ottica di miglioramento continuativo.

*Tabella 12 Processo di gestione e controllo delle criticità*

| **Soluzioni per la flessibilità e tempestività nell'allocazione risorse** |
|---|
| **1. INDIVIDUAZIONE CRITICITÀ.** In tale fase, il costituito RTI prevede la tempestiva individuazione degli eventi in grado di influenzare il regolare svolgimento dei servizi (ad es. picchi di attività, concentrazione tempistiche, cicli di reworking, etc.). In particolare, in funzione delle tipologie dei vari interventi pianificati e della loro complessità, il costituito RTI fornirà un supporto strutturato continuo per l'individuazione e la valutazione predittiva delle criticità. Questa attività sarà ripetuta a seguito dei controlli di avanzamento operativo delle attività di migrazione, oppure in risposta a situazioni improvvise rilevate. |

**2. VALUTAZIONE IMPATTI**. In tale fase, il costituito RTI analizza ed esamina gli eventi identificati nella prima fase, con particolare attenzione a tutti gli eventi "critici" di maggiore impatto e probabilità. Particolare attenzione viene, infatti, data in questa fase all'analisi di nuove esigenze, identificate nella fase 1, in termini di staffing. Con riferimento a queste ultime, il costituito RTI valuterà il numero di risorse necessarie per l'esecuzione delle attività e le competenze richieste per contenere la magnitudo dell'evento. In caso di necessità si procederà a:




- quantificare e tempificare l'aumento o la diminuzione delle risorse;
- determinare la variazione del mix di figure professionali;
- ricomporre/variare i profili di competenza all'interno di ogni Team;
- identificare il profilo delle nuove risorse necessarie o le risorse da rilasciare;
- definire eventuali variazioni della struttura del team di lavoro (es. creazione di "task force" per lo svolgimento in tempi brevi di attività critiche o l'organizzazione di pool di esperti/risorse molto specializzate per supporti mirati ad attività in corso).

Una volta identificati e analizzati, tali eventi vengono valutati sulla base della prevedibilità di accadimento e del relativo impatto sugli incarichi di lavoro; a seguito di tale valutazione gli eventi vengono posizionati su una specifica "Matrice degli Eventi" che, in funzione del grado di prevedibilità dell'evento e del relativo impatto sui carichi di lavoro, consente di definire le risposte organizzative più opportune. In particolare, l'approccio proposto presuppone l'identificazione di 4 scenari possibili (i 4 quadranti matrice) con le soluzioni organizzative più opportune, come di seguito rappresentato:

**Quadrante 1 - Gestione "ordinaria"** |*Eventi con limitato impatto, ma con basso grado di prevedibilità*

Tali eventi possono essere indirizzati con gli strumenti di gestione ordinaria del progetto, come ad es.: ⊠ Previsione, nella programmazione ex ante, di appositi "cuscinetti" temporali in grado di limitare l'impatto dell'evento critico; ⊠ Riallocazione parziale delle attività tra le figure professionali impegnate nel progetto.

**Quadrante 2 – Fine tuning programmazione** |*Eventi con limitato impatto ed agevolmente prevedibili*

Tali eventi possono essere indirizzati tramite una revisione della programmazione operativa delle attività. Per la corretta gestione di tali eventi sarà opportuno: ⊠ Ripianificare le attività, provvedendo ad una ridefinizione parziale del piano di migrazione; ⊠ Valutare la necessità di riallocare le risorse su nuove attività; ⊠ Intensificare

gli incontri periodici tra i Referenti Tecnici del costituito RTI e i Referenti dell'amministrazione al fine di verificare costantemente l'allineamento tra il Piano di Lavoro (attività, tempi, risorse, metodologie) e le priorità di progetto.

**Quadrante 3 – Pianificazione |***Eventi altamente prevedibili e con forte impatto*

Tali eventi possono essere affrontati con strumenti di pianificazione straordinaria quali: ⊠ Ridefinizione complessiva della pianificazione delle attività di migrazione; ⊠ Inserimento nel team di nuove risorse aggiuntive e/o modifica del mix dei profili professionali; ⊠ Shift di risorse tra un team e l'altro, previa verifica di sostenibilità complessiva; ⊠ Pianificazione di incontri ad-hoc tra i Project Manager del costituito RTI, i Technical Leader del costituito RTI e i Referenti dell'Amministrazione

**Quadrante 4 – Recovery Plan |***Eventi imprevedibili e con forti impatti*

Tali eventi dovranno essere fronteggiati con un *Recovery Plan*. Al verificarsi dell'evento, l il costituito RTI si impegna ad avviare immediatamente, di concerto con l'Amministrazione le seguenti attività: ⊠ Modifica sostanziale del mix di figure professionali presenti sul progetto; ⊠ Costituzione ed attivazione, a richiesta, di task force dedicate a nuove linee di attività; ⊠ Ricorso ad esperti esterni o appartenenti al *network* nazionale, qualora siano richieste competenze specifiche inizialmente non previste.

**3. IDENTIFICAZIONE E PIANIFICAZIONE AZIONE CORRETTIVA.** L'analisi svolta tramite le fasi 1 e 2 termina con lo studio del potenziale impatto dell'evento critico su una intera fase progettuale e la conseguente azione correttiva. A valle della valutazione, il costituito RTI elaborerà un brief contenente le seguenti informazioni principali: la descrizione dell'evento identificato e relativa classificazione; la valutazione dei relativi impatti sugli obiettivi di progetto; lista delle possibili azioni correttive ed eventuali "effetti collaterali" delle stesse, compresa la pianificazione ed il dimensionamento delle risorse per ogni azione correttiva individuata. Il costituito RTI provvederà a condividere tale Relazione con **l'Amministrazione affinché approvi la specifica azione e soluzione organizzativa proposta.**

**4. ESECUZIONE.** Sulla base della soluzione approvata dall'Amministrazione in merito alle specifiche azioni da attuare, il costituito RTI provvederà ad implementare, monitorare e controllare le soluzioni organizzative/azioni correttive identificate. Con riferimento alla gestione del Team di lavoro, in questa fase le risorse individuate sono immediatamente contattate ed aggiornate sui contenuti del progetto, così da diventare rapidamente operative. Contemporaneamente, sono implementate tutte le modifiche organizzative alla struttura dei Gruppi di lavoro atte a garantire la massima efficacia dell'inserimento.

**5. VALUTAZIONE POST ESECUZIONE.** In questa ultima fase, il costituito RTI analizzerà l'efficacia delle azioni e delle soluzioni implementate in termini di benefici ottenuti rispetto alle risorse utilizzate. Più in dettaglio, si predisporrà un **Report conclusivo** volto ad illustrare I risultati derivanti dall'applicazione delle soluzioni

proposte. Sulla base di questa valutazione, e delle *lesson learned*, si continuerà a monitorare il manifestarsi di eventi critici in un'ottica di miglioramento continuo.

## 23.4 Strumenti

Come elemento migliorativo per la gestione e il monitoraggio della presente fornitura, il costituito **RTI prevede l'utilizzo di una serie di strumenti dedicati**. Gli strumenti si intendono erogati tramite il Portale della Fornitura, implementato dal costituito RTI.

Tabella 13 Strumenti per gestione e monitoraggio della fornitura

| Strumento | Metodologia di riferimento | Descrizione |
|---|---|---|
| Masterplan | Gestione del Portfolio | Cruscotto dedicato al monitoraggio del Portfolio di Iniziative di Migrazione |
| Planner risorse | Gestione delle Risorse | Dashboard su piattaforma MS Excel che garantisce la corretta allocazione delle risorse ingaggiate a seconda di competenze ed effort stimato e consuntivato |
| Piano di Progetto | Monitoraggio e Controllo del Progetto | Strumento basato su MS Project, dedicato al monitoraggio di tutte le attività e deliverable della singola Iniziativa |
| Cruscotto Monitoraggio Avanzamento | | Cruscotto parametrico basato su MS Excel da utilizzare al fine di monitore le attività di migrazione |
| Issue Log | | Strumento a supporto del monitoraggio delle Issue emerse e delle potenziali strategie di risposta |
| KPI Monitoring Dashboard | Monitoraggio Performance (KPI) | Dashboard implementata tramite MS Power BI tramite cui monitorare i KPI di migrazione con viste dinamiche |
| Strumenti di Gestione dei Rischi | Gestione dei Rischi | Cfr. ID 22 |
| Tool e tecnologie di migrazione | | |
| Piano di Change Management | Change Management e Formazione | Pianificazione delle attività di Change Management direttamente collegate alle Iniziative di migrazione |
| Report di Change Management | | Documentazione sviluppata con cadenza custom a seconda delle esigenze, riportante i principali risultati raggiunti |

Si presenta di seguito una breve descrizione degli strumenti indicati in Tabella 13.

### 23.4.1 Masterplan

Il Masterplan è un documento di sintesi che riporta tutte le **Iniziative di migrazione a livello di portfolio**, aggiornato con cadenza mensile (o comunque tempestivamente in base delle nuove esigenze derivanti dalle attività progettuali); contiene tutte le informazioni che riguardano le **iniziative di migrazione sia pianificate sia in corso**. Le iniziative sono rappresentate in un GANTT che include tutte le variabili utili al monitoraggio delle attività di progetto e alla loro analisi proattiva. Le informazioni includono: pianificazione temporale dei task, stato di avanzamento, owner, milestone, deliverable, economics associati, criticità, azioni di rientro proposte, nonché informazioni su eventuali non conformità e/o mancate accettazioni del servizio/prodotto. La Figura 46 riporta un esemplificativo della vista aggregata di 4 Iniziative di Migrazione, con le relative milestone e deliverable, articolate nel corso di un anno; la pagina sarà **navigabile ed espandibile** sia nel tempo che nelle Iniziative, prevedendo un **collegamento** dinamico alla vista di dettaglio della singola Iniziativa prevista dallo strumento "**GANTT di Progetto**". Il Masterplan rappresenta un efficace strumento di **reporting di Alto Livello** a disposizione del management, consentendo il monitoraggio efficace di tempi e costi rispetto alle singole attività operative, nonché criticità e aspetti finanziari ed economici di massima, e garantendo inoltre una maggiore efficienza nell'applicazione dinamica di Change ai Piani di Progetto laddove si dovessero rendere necessarie modifiche e/o ottimizzazioni.

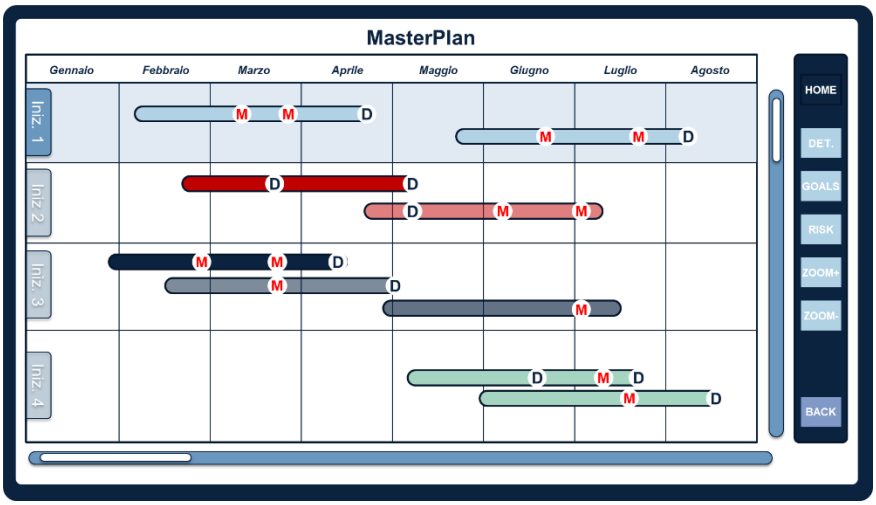



**Figura 46 MasterPlan iniziative esemplificativo**

### 23.4.2 Planner risorse

Per supportare una corretta gestione delle risorse, il costituito RTI impiegherà un tool di *Workforce e Workload Management,* in grado individuare il match ottimale tra le competenze necessarie ad eseguire le richieste dell'Amministrazione ed il dimensionamento ottimale per l'esecuzione delle singole attività. Il *tool* è comprensivo di una mappa delle competenze delle risorse proposte dal costituito RTI e del *workload* in essere per ogni singola risorsa. Il tool sarà a supporto del pillar delle modalità operative, operando sui 5 step descritti a livello di metodologie. In particolare, nella definizione dei volumi di attività

e nella raccolta esigenze. Il tool include inoltre i criteri di staffing basati sulle competenze delle singole risorse e per la costruzione del mix di professionalità da impiegare sull'iniziativa. In ultimo, al fine di evitare eventuali sovra o sotto allocazioni, il tool consente di verificare la disponibilità delle risorse in tempo reale.

### 23.4.3 Piano di Progetto

Tale strumento orchestra tutte le funzionalità di pianificazione e governance, permettendo di raggiungere gli obiettivi istituzionali e strategici dell'Amministrazione legati ai processi di migrazione in Cloud. In particolare, lo strumento permette di pianificare, seguire e formalizzare quanto definito in termini di pianificazione delle singole attività. Agli utenti che accederanno a questa area del Portale sarà fornito un **efficace strumento di riferimento per monitorare la pianificazione degli interventi e le evoluzioni in corso d'opera** degli stessi, in modo tale da garantire la massima efficienza della conduzione tecnica ed operativa delle attività. In questa sezione sarà presente un **diagramma** di **Gantt** sempre aggiornato con l'immediata visualizzazione delle interdipendenze tra le attività e le date di scadenza/milestone da gestire per il progetto di migrazione, visualizzando in maniera semplice e immediata metriche di misurazione quali lo scostamento dalla pianificazione.

Le principali caratteristiche funzionali dello strumento per gestire le funzionalità di pianificazione di dettaglio (WBS, GANTT) sono:

- sintesi e dettaglio di tutte le iniziative in corso e pianificate;
- valutazione dello stato di avanzamento (delle attività e del budget) di ogni singola iniziativa;
- individuazione delle iniziative critiche;
- definizione dei piani di recupero.

Attraverso questo strumento sarà dunque possibile:

- impostare la Pianificazione iniziale;
- controllare le attività di progetto, anche nel merito delle tematiche economiche e professionali (es. impiego FTE per la singola attività);
- articolare e dettagliare il piano di lavoro del progetto;
- controllare l'avanzamento rispetto alle tempistiche;
- produrre in modo automatico una serie di report direzionali;
- gestire la consegna di deliverable di fornitura e output associati.

### 23.4.4 Cruscotto Monitoraggio Avanzamento

Al fine di **monitorare efficacemente** non solo il progresso delle attività di migrazione dal punto di vista delle risorse impiegate (sia economiche, che a professionali), ma anche l'**avanzamento tecnico** delle varie fasi di passaggio al Cloud, il costituito RTI metterà a disposizione un **cruscotto di monitoraggio** a livello di **singola iniziativa**. Tale strumento è specificamente costruito per dare un'overview complessiva e sintetica delle fasi della migrazione, utilizzando un **sistema parametrico** al fine di normalizzare le informazioni afferenti a applicativi di dimensioni eterogenee.

Tale sistema assegna un **peso a ciascuna fase**, dipendente dall'effort rispetto all'intero progetto. I pesi proposti sono riportati nella figura sottostante:

| Fase di Migrazione | Peso Relativo |
|---|---|
| Analisi/Discovery | 30% |
| Setup | 20% |
| Migrazione | 40% |
| Collaudo | 10% |

**Figura 47 Pesi relativi per le varie fasi di migrazione**

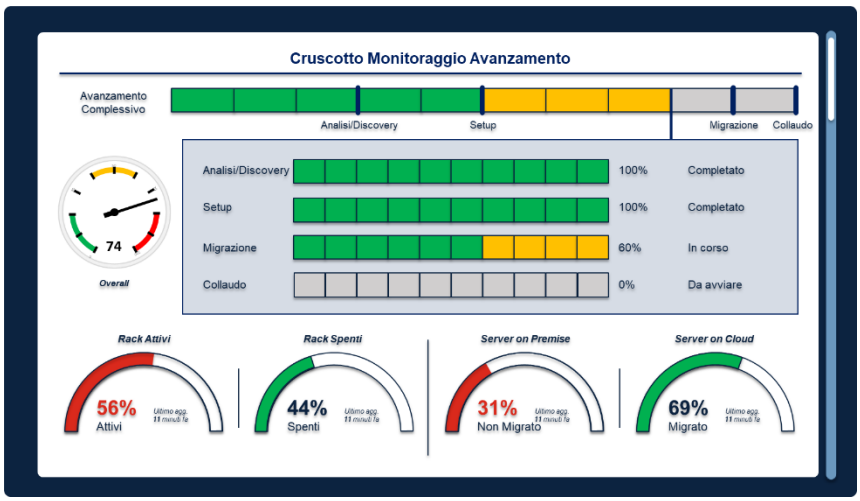



**Figura 48 Cruscotto monitoraggio avanzamento**

Inoltre, per ciascuna fase, verrà misurato l'avanzamento di dettaglio, in modo da distillare ulteriormente le informazioni sullo stato delle attività. Ad esempio, per la fase di migrazione sarà possibile determinare quanto del 40% del peso della fase è stato raggiunto, attraverso il conteggio di alcuni indicatori tecnici specifici per la fase. Nel caso della migrazione, ad esempio, sarà possibile misurare il numero di server/rack che sono stati spenti e migrati in cloud, andando a definire una percentuale sul totale di server/rack oggetto di migrazione. Ancora, per la fase di collaudo, sarà misurato un avanzamento percentuale calcolando i test condotti con esito positivo rispetto al totale dei test da condurre, tenendo anche conto degli impatti di eventuali test condotti con esito negativo.

### 23.4.5 Issue Log

L'Issue Log è un documento a supporto del monitoraggio e del controllo del progetto, dove vengono aggregate tutte le issue che emergono durante le attività di migrazione. Sviluppato su una griglia opportunatamente condivisa e messa a disposizione dell'Amministrazione e del costituito RTI, registra le issue attraverso un codice univoco, identificando la causa che lo ha generato, l'impatto espresso in ore o gg/uu di ritardo, il livello di rischio collegato alla singola issue. Inoltre, sia per finalità di tracciamento che per contribuire alla condivisione di conoscenze e best practice all'interno delle diverse iniziative di migrazione, ad ogni issue è associata anche la strategia di risposta adottata, in modo da consentire ad altri gruppi di lavoro che affrontano problematiche uguali o assimilabili di poter utilizzare le stesse pratiche già impiegate in precedenza.

**Issue Log**

| ID | Issue | Causa | Impatto | Livello di Rischio | Strategia di Risposta |
|---|---|---|---|---|---|
| 1 | Ritardo fine implementazione infrastruttura | Mancato completamento adeguamento rete | 200-250 ore di ritardo | Alto | Procedere con l'adeguamento Infrastruttura delle altre componenti del Cluster |
| 2 | Ritardo Adeguamento Rete | Moduli non pronti | 400-500 ore di ritardo | Medio | Richiedere con urgenza e monitorare |
| 3 | Complicazioni di tipo burocratico in fase di selezione CSP | Indisponibilità piattaforma selezione CSP | 80-120 ore di ritardo | Basso | Monitorare e compilare un reclamo al gestore della piattaforma |
| 4 | Impedimento nel completare la Wave | Sincronizzazione nel cluster non perfezionata | 150-200 ore di ritardo | Medio | Minimizzare tempi di attesa iniziando a perfezionare aspetti post-migrazione |

**Figura 49 Issue Log e strategie di risposta**

### 23.4.6 Tool e Tecnologie di Migrazione

L'ATI, al fine di contenere i rischi direttamente connessi alle attività di migrazione, sulla base delle proprie Best Practices adotterà l'uso di strumenti e tecnologie allo stato dell'arte per favorire in tempi, modi e sicurezza le attività oggetto della fornitura. Come già descritto in ID 20 "Miglioramento delle modalità per la migrazione in cloud - Risorse e tempistiche" ciascuno progetto di on-boarding prevede uno studio di dettaglio per analizzare l'ambiente sorgente e le eventuali attività di remediation che devono essere fatte per poter migrare le VM.

Gli strumenti in uso al RTI permetteranno diverse tipologie di migrazione sulla base delle tecnologie che adottano i sistemi all'Amministrazione. Ogni tipologia farà riferimento ad una matrice di compatibilità relativa alla configurazione della singola VM che deve essere migrata (Bulk Migration, Live Migration, Cold migration). In questo contesto, la maturità "tecnologica" dell'Amministrazione ricopre un ruolo determinante nella scelta della tipologia di migrazione, ma sarà in ogni caso garantito il minor impatto possibile sui tempi di fermo dei servizi, sicurezza nello spostamento degli stessi e possibilità di rollback con impatti minimi, in caso di necessità.

Per il dettaglio degli strumenti e delle tecnologie relativi alle attività di migrazione, si rimanda all'ID 20, dove sono illustrate nel dettaglio le diverse tipologie di configurazione.

### 23.4.7 KPI Monitoring Dashboard

Il modulo del Portale della Fornitura "Sistema di Monitoraggio dei KPI "è composto da una **serie di dashboard e cruscotti**, attraverso cui sarà possibile visualizzare, per ciascuna migrazione, un'**alberatura a più livelli**, partendo dai KPI di aggregazione e consentendo agevolmente il drill down fino al singolo indicatore di impatto o di risultato. Il sistema ovviamente consta al suo interno degli **indicatori e delle formule per calcolarli**, delle logiche di aggregazione e delle varie viste che è possibile presentare all'utente.

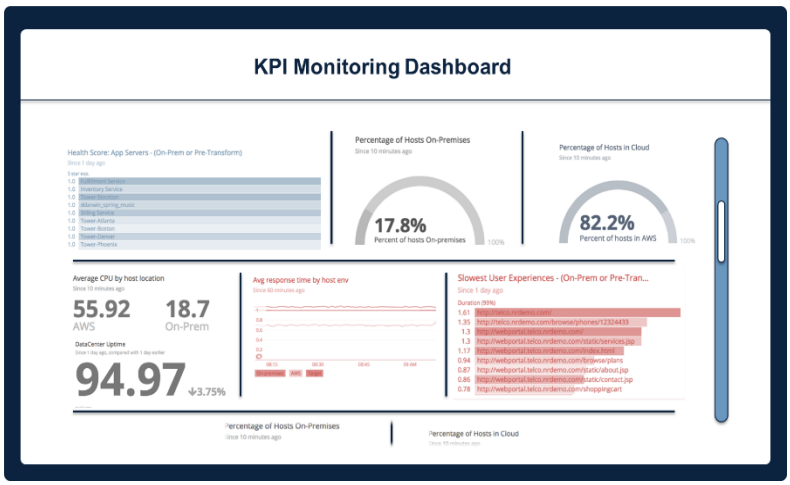



**Figura 50 Dashboard di monitoraggio KPI esemplificativa**

Il sistema di rappresentazione consente la **facile lettura di ciascun dato**, integrando gli elementi grafici con informazioni e descrizioni. È inoltre possibile suggerire all'utente che sta visualizzando una determinata area una serie di indicatori correlati. Il sistema, come già accennato, consente di supportare una **governance ottimale del processo di migrazione**, rappresentando non solo una valutazione dello stato iniziale, ma anche monitorando l'andamento della migrazione, ed è in grado di valutare i benefici e gli impatti realmente raggiunti al termine del processo.

### 23.4.8 Piano di Change Management

Il tool permette di gestire il cambiamento introdotto dal programma/progetto di migrazione, attraverso la **definizione e la gestione del Piano di Change Management**, nel quale sono riportati tutti gli interventi a livello organizzativo, di comunicazione e di formazione necessari per adeguare il contesto cliente e gli attori coinvolti (es. piani di formazione, revisione dei modelli operativi o dei processi). Lo strumento mette a disposizione, laddove necessario, un modulo per la valutazione delle competenze rispetto al cambiamento intrapreso, al fine di determinare la necessità di eventuali piani di formazione ad-hoc.

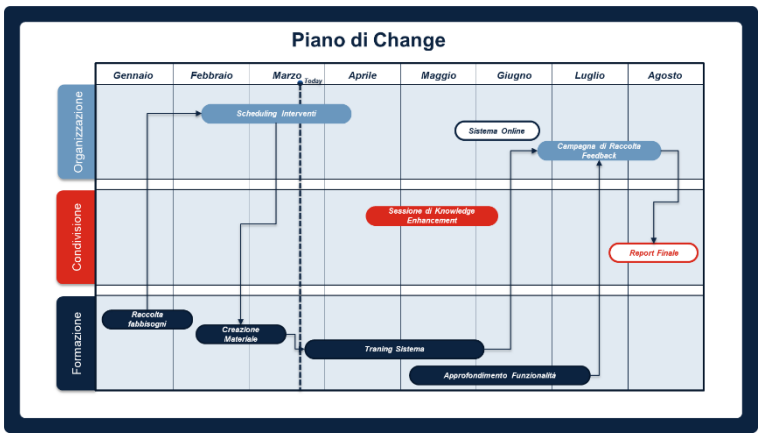



**Figura 51 Piano di Change esemplificativo**

### 23.4.9 Report di Change Management

Il report di Change Management è prodotto ad intervalli predeterminati (se richiesto) oppure al completamento del Piano di Change, riassumendo i **principali step intrapresi nel processo di cambiamento**, evidenziando eventuali **criticità emerse** e le soluzioni impiegate per affrontarle, in ottica di riuso e condivisione delle "**lesson learned**".

# 24 ID 22 – Valutativo - Miglioramenti della strategia di mitigazione dei rischi connessi alla migrazione dei servizi delle amministrazioni (disponibilità, integrità e performance)

## 24.1 Executive Summary

Il Costituito ATI, in linea con quanto richiesto dal Criterio ID 22, in relazione alla premialità legata alla mitigazione dei rischi connessi alla migrazione in cloud, tratterà il tema del miglioramento della strategia di mitigazione dei rischi connessi alla migrazione in cloud evidenziando gli elementi di processo di risk management introdotti a tal scopo, con la consapevolezza di aver realizzato una soluzione progettuale che integra elementi di infrastruttura, modelli e strumenti che minimizzano sia i rischi connessi alle fasi propriamente di migrazione dei servizi in cloud, sia quelli potenzialmente connessi al servizio già migrato.

Di seguito sono illustrate le tematiche e le attività evidenziate nella seguente mappa concettuale (Figura 52), messe in campo al fine di mitigare i rischi di disponibilità, integrità e performance legati alla migrazione dei servizi delle amministrazioni richiedenti.

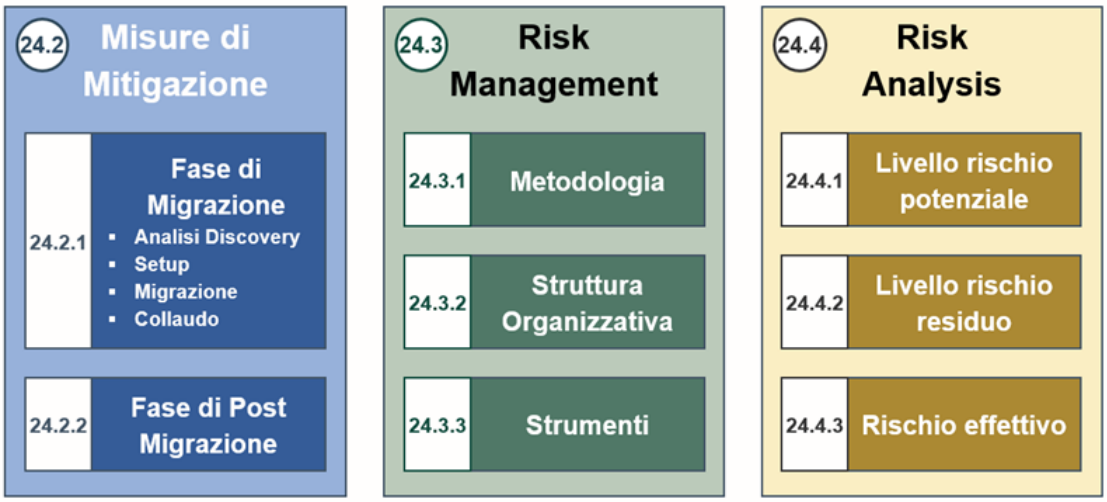



**Figura 52 Mappa concettuale**

Le principali tematiche affrontate riguardano:

- **misure di mitigazione** proposte sia nella fase di migrazione, sia in quella di post migrazione e hand over del servizio, che saranno dettagliate nel primo capitolo, che riguarderanno:
  - **processi**, per ottimizzare la raccolta delle informazioni e vincoli sui servizi da migrare, dimensionare l'ambiente target e pianificare al meglio l'esecuzione del lift&shift o del re-architecting delle applicazioni;
  - **strumenti,** a supporto della migrazione logica dei servizi e del testing;
  - **standard documentali,** per facilitare la collaborazione tra il Team di lavoro e Stakeholder dell'Amministrazione;
- **metodologia di Risk Management** che sarà adottata durante tutto il progetto di migrazione: la descrizione, presente nel secondo capitolo, darà evidenza sia dell'Organizzazione, che degli Strumenti utilizzati dal costituito RTI. In particolare, nel capitolo dedicato, saranno approfondite le fasi in cui si articola tale metodologia;
- **metodologia di Risk Analysis,** che sarà dettagliata nel terzo capitolo, che si articolerà in:
  - **calcolo del livello di esposizione al rischio potenziale** delle attività di Migrazione, nel caso non siano adottate misure di mitigazione descritte nel primo capitolo;
  - **calcolo del livello di esposizione al rischio residuo** delle attività di Migrazione, nel caso sia adottato un set standard di misure di mitigazione descritte nel primo capitolo;

- **calcolo del rischio effettivo** delle attività di Migrazione in funzione del valore che i servizi migrati hanno per gli utenti interni ed esterni dell'Amministrazione;

La soluzione proposta dal costituito RTI è caratterizzata dai seguenti punti di forza:

- La metodologia è fortemente incentrata sulla mitigazione delle tre tipologie di rischi identificati:
  - disponibilità;
  - integrità;
  - performance;
- Un approccio integrato e trasversale alle quattro fasi standard di una Migrazione (Analisi/Discovery, Setup, Migrazione, Collaudo), in modo che i rischi siano prontamente identificati, monitorati e mitigati;
- Un continuo e trasparente coinvolgimento degli Stakeholder dell'Amministrazione, che avranno visibilità sia dei rischi, sia delle strategie di mitigazione;
- Un approccio basato sulla metodologia Agile (Scrum, DevOps) in linea con le più recenti best practices adottate in queste tipologie di progetti;
- Un approccio iterativo e incrementale al fine di semplificare la gestione e mitigazione del rischio e coprire l'intero ciclo di vita del progetto;
- L'Adozione di metodologie di Continuous Improvement e Consolidamento della Knowledge, in modo che ogni Lesson Learned appresa in una fase iterativa, permetta il tuning e l'ottimizzazione dell'iterazione successiva.
- Aderenza a quanto indicato dall'AgID nelle sue linee guida sulla Migrazione al Cloud.

Alcune delle scelte strategiche effettuate in fase di soluzione di progetto, e principalmente infrastrutturali, per indirizzare il tema della mitigazione dei rischi, possono essere così riassunte:

- **Posizione geografica delle Region**: la vicinanza geografica alle principali Pubbliche Amministrazioni minimizza sia impatti logistici, sia tecnologici, quali ad esempio quelli legati alle latenze sulle tratte che rendono fruibili i servizi in cloud;
- **Posizione geografica dei Data Center all'interno della Region**: la posizione reciproca dei due DC all'interno della stessa Region è ottimale, alla distanza sufficiente per sopperire ad un congruo numero di eventi di disastro di carattere localizzato, ma anche sufficientemente prossimi per poter garantire tempi di latenza di rete Round Trip dell'ordine di grandezza del **millisecondo;** questi valori di latenza sono idonei a recepire un utilizzo dei DC in modalità Active/Active e quindi pronti ad ospitare qualsiasi tipologia di casi d'uso;

- **Posizione geografica dei Data Center tra differenti Region**: la posizione reciproca dei DC tra Region diverse è ottimale per poter garantire resilienza ad un congruo numero di eventi di disastro, ma anche per poter garantire bassi tempi di latenza di rete Round Trip**;** questi valori di latenza sono idonei a recepire scenari di DR per un numero vastissimo di casi d'uso;
- **Posizione geografica di tutti i data center**: dislocati in zone sismiche 3-4 e quindi a basso rischio, in posizioni strategiche rispetto ad aeroporti internazionali dai quali sono facilmente raggiungibili;
- **Gestione dei piani di continuità**: grazie ad un team specificamente dedicato alla gestione dei piani di continuità, le strategie di Business Continuity e Disaster Recovery vengono continuamente sottoposte ad audit e revisionate, verificando inoltre, secondo il processo di Continual Service Improvement, il costante allineamento di metodologie e strumenti in uso rispetto allo stato dell'arte. In quest'ottica, il processo di revisione continuo include anche la Business Impact Analysis, ovvero l'analisi degli aspetti funzionali dei servizi che ne determinano la criticità e quindi il relativo inquadramento nelle strategie di BC/DR, verificando se, a fronte di eventuali evoluzioni dei servizi e delle relative applicazioni, siano state effettivamente aggiornate le corrispondenti strategie di BC o DR: ciò riduce il rischio che le soluzioni correnti si discostino dalle effettive esigenze funzionali del servizio, riducendo quindi il rischio di indisponibilità del servizio stesso.

La soluzione progettuale abilita inoltre a recepire, in ottica evolutiva, modelli migliorativi di:

- **Monitoraggio prestazionale a livello applicativo**: nell'ambito della gestione applicativa specifica dell'Amministrazione, è possibile ottimizzarla sfruttando un monitoraggio applicativo e prestazionale (APM – *Application Performance Monitoring*) dei principali KPI funzionali dei servizi, che intercettano potenziali degradi prestazionali a livello applicativo e che possono anche portare all'indisponibilità del servizio. Inoltre, grazie a strumenti abilitanti la correlazione degli eventi, e con piattaforme di Machine Learning, si riescono ad intercettare in maniera predittiva specifici pattern del carico di lavoro e del comportamento applicativo, che annunciano il degrado del servizio stesso; in questo modo gli eventi vengono anticipati e possono essere condotte azioni di *remediation*.

È noto che le fasi di migrazione delle applicazioni e dei servizi sono ad altissima complessità, oggetto di una non trascurabile percentuale di insuccessi. Il rischio che questo avvenga è mitigato non solo da processi di risk management ben pensati e strutturati, non solo da infrastrutture e strumenti allo stato dell'arte, ma anche da gruppi di lavoro costituiti da skill di elevato profilo, dimostrabile sia attraverso

esperienze pregresse in contesti analoghi e sia attraverso percorsi di certificazione tecnica in linea con le piattaforme previste in uso al PSN. Il costituito RTI prevede quindi un utilizzo massiccio di profili con certificazioni tecniche complessive rese disponibili in ambito PSN.

## 24.2 Misure di Mitigazione

Data l'esperienza delle Partecipanti al costituito RTI in ambito migrazione al Cloud, questo possederà una Knowledge consolidata sui rischi a cui si può incorrere in tale tipologia di progetti, che possono essere suddivisi nelle seguenti categorie logiche:

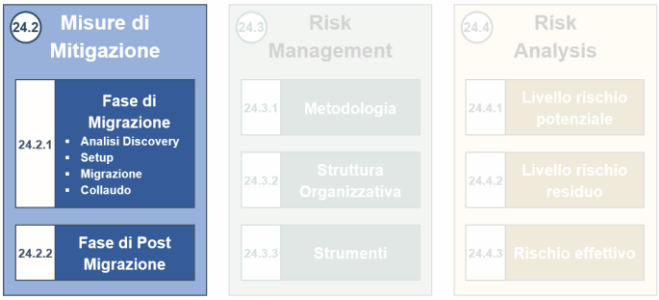



**Figura 53 Focus Misure di Mitigazione**

- **Relation**, connessi a un inadeguato commitment dei team applicativi e degli Stakeholder dell'Amministrazione, dipendente da cause legate a una non corretta organizzazione dei gruppi di lavoro e dal design errato dei protocolli/processi di comunicazione e di collaborazione;
- **Knowledge**, legati ai gap informativi del team di progetto sull'infrastruttura di origine e sui servizi da migrare, che a loro volta si suddividono in due diverse sottocategorie:
  - **Fog,** dovuta a una non completa conoscenza dell'ambiente da migrare conseguenza, ad esempio, di una documentazione non aggiornata o a lacune nell'esecuzione dell'Assessment;
  - **Sudden,** dovuta a imprevisti che emergono durante la Discovery dell'ambiente da migrare. Esempio concreto, l'esistenza di IP cablati nei codici sorgenti delle applicazioni, che possono trasformare una migrazione da lift and shift a una di rearchitect, incrementando sia le tempistiche, sia gli effort necessari al progetto;
- **Setting**, legati a un inadeguato design e/o dimensionamento della piattaforma target della migrazione, rendendo così non raggiungibili gli SLA e/o i KPI condivisi con l'Amministrazione;
- **Planning,** legati a una non adeguata scelta della strategia di migrazione e/o pianificazione, creando dei disservizi legati al non rispetto dei vincoli di dipendenza applicativa;
- **Integrità,** relativi ad esempio alla perdita di informazioni, gli errori di semantica (incoerenza tra campi di partenza e destinazione);
- **Disponibilità**, relativi ad esempio a un eventuale downtime dipendente dalla strategia di migrazione scelta o da una sua errata orchestrazione;

- **Performance**, relativi ad esempio a un'instabilità delle applicazioni migrate nel nuovo ambiente o a un non corretto dimensionamento delle risorse computazionali ad esse associati.

Le categorie con cui sono classificati i rischi non sono tra loro indipendenti, ma legate in relazione modellizzabile con una specifica struttura ad albero, evidenziata nella figura seguente:

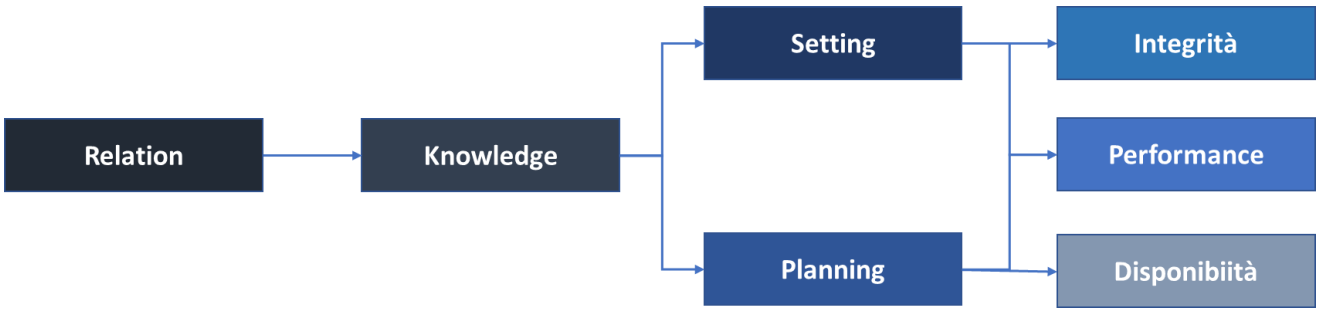



**Figura 54 Relazione tra i rischi**

La consapevolezza di questa relazione ha permesso al costituito RTI di definire un modello concreto di mitigazione del rischio, le cui specifiche misure descritte nei paragrafi successivi saranno focalizzate a minimizzare probabilità di accadimento e di impatto di tali categorie, secondo la tabella seguente che evidenzia la correlazione tra i rischi principali coperti nelle varie fasi di Migrazione.

Tabella 14 Modello di mitigazione del rischio

| | Fase di Migrazione | | | | Post Migrazione |
|---|---|---|---|---|---|
| | Analisi/Discover | Setup | Migrazione | Collaudo | |
| Relation | ✓ | | | | |
| Knowledge | ✓ | | | | |
| Setting | | ✓ | | | ✓ |
| Planning | ✓ | | | | |
| Performance | ✓ | ✓ | ✓ | ✓ | ✓ |
| Disponibilità | ✓ | ✓ | ✓ | ✓ | ✓ |
| Integrità | ✓ | ✓ | ✓ | ✓ | ✓ |

### 24.2.1 Misure di mitigazione adottate per ciascuna fase della migrazione

Di seguito verranno approfondite, a titolo esemplificativo, le attività svolte ed i rischi più comuni che si possono incontrare durante tutte le fasi di un progetto di migrazione. Un preciso tracciamento dei rischi ed una corretta esecuzione di queste azioni consentono di garantire la disponibilità, integrità e le performance degli ambienti migrati. Verranno pertanto valutati gli impatti attesi derivanti dai rischi di disponibilità, integrità e performance secondo la seguente scala.




**Figura 55 Focus Fase di Migrazione**

Tabella 15 Legenda valutazione impatti

| | |
|---|---|
| **Basso impatto** | |
| **Medio impatto** | |
| **Alto impatto** | |

#### 24.2.1.1 *Analisi/Discovery*




La fase di Analisi/Discovery ha l'obiettivo di analizzare i workload/servizi esistenti che dovranno essere migrati e di ottenere tutte le informazioni necessarie per determinare il tipo di migrazione, il livello di impegno e i gruppi di applicazioni. I rischi più comuni in tale fase sono legati ai successivi ambiti:

- **Knowledge**, con un'errata e/o incompleta conoscenza dell'ambiente da migrare, dei vincoli operativi e delle specifiche esigenze dell'Amministrazione, che potrà impattare a regime sui parametri richiesti di disponibilità, di performance e di integrità;
- **Relation**, non coinvolgendo adeguatamente nei processi di Analisi/Discovery gli stakeholder dell'Amministrazione;
- **Planning,** diviso in:
  - **Timing**, con un incremento delle tempistiche necessario all'assessment;
  - **Wave planning**, con un'errata e/o incompleta identificazione delle dipendenze tra i bundle da migrare, creando a regime un disservizio all'Amministrazione, impattando sui criteri di performance e sulla disponibilità;
- **Performance**, relativa alla comprensione del funzionamento ottimale dell'infrastruttura target;

- **Disponibilità**, fornisce un'indicazione su cosa migrare e come farlo in maniera omogenea per evitare malfunzionamenti (ad esempio dovuti a migrazioni incomplete rispetto ad alcuni componenti specifici);
- **Integrità**, consiste nella verifica di consistenza e qualità dei dati per verificare adesione agli standard da garantire.

Come specifica attività di mitigazione, il costituito RTI ha definito un processo specifico articolato in cinque punti:

- **Riunione di Start-up,** finalizzata alla mitigazione dei rischi di relation e alla definizione congiunta dell'organizzazione e dei processi tra team di progetto e Stakeholder dell'Amministrazione, per facilitare le attività di migrazione;
- **KPIs,** utilizzati per il monitoraggio dell'avanzamento delle fasi realizzative in linea con i requisiti di progetto per mitigare i rischi di Performance, Disponibilità e Integrità;
- **Assessment**, che per minimizzare i rischi di **Knowledge** e di **Timing**, potrà, se ritenuto opportuno dall'Amministrazione, svolgersi tramite la metodologia Scrum;
- **Wave Planning,** per pianificare la scaletta di migrazione sulla base delle interdipendenze applicative individuate tra i sistemi oggetto di migrazione e per la definizione della corretta strategia della coesistenza degli ambienti dell'Amministrazione fino al completo spegnimento dell'infrastruttura sorgente;
- **Risk Analysis**, di dettaglio del singolo progetto, che si svolgerà secondo la metodologia descritta in precedenza, che a seconda della complessità individuata, potrà essere svolta dal PMO o da un componente del Risk & Issue Management Team. Il processo sarà articolato in tre fasi
    - **Fase 1: dedicato alla presentazione, validazione e fine tuning delle ipotesi iniziali riguardanti i rischi della migrazione e delle relative strategie di mitigazione;**
    - **Fase 2: dedicata all'implementazione della metodologia di risk analysis;**
    - **Fase 3: dedicata alla stesura del Piano di Mitigazione Rischi e Contingency Plan.**

Di seguito viene evidenziata la stima, che dovrà essere contestualizzata a seconda del progetto e della singola Amministrazione, di come le attività di mitigazione previste nella fase di Analisi/Discovery impattino, mitigandoli, i rischi di disponibilità, integrità e performance.

*Tabella 16 Valutazione impatti Analisi/Discovery*

| | Disponibilità | Integrità | Performance |
|---|---|---|---|
| Riunione di Start Up | ● | ● | ● |
| KPIs | ● | ● | ● |
| Assessment | ● | ● | ● |
| Wave Planning | ● | ◔ | ◑ |
| Analisi dei rischi | ● | ● | ● |

#### 24.2.1.2 *Setup*




Analogamente a quanto evidenziato nella fase di Analisi/Discovery, anche per la seconda fase di Setup è condivisa di seguito la stima, che ovviamente dovrà essere contestualizzata a seconda del progetto e della singola Amministrazione, di come le attività di mitigazione previste impattino sui rischi relativi a Disponibilità, Integrità e Performance:

Tabella 17 Valutazione impatti Setup

| | Disponibilità | Integrità | Performance |
|---|---|---|---|
| Landing Key Value | ◑ | ◑ | ● |
| Migrazione Pilot e Lesson Learned | ● | ● | ◔ |

I rischi più comuni in tale fase sono legati a tre ambiti:

- **Disponibilità**, insufficiente potenza computazionale dovuto a stime preliminari al processo errate;
- **Integrità,** collegamenti con altre applicazioni non considerati e quindi non incluse nella migrazione (ad esempio, collegamenti con libreria);
- **Performance**, capacità computazionali e/o livello di servizio degradato durante il processo di migrazione, risultando in prestazioni inferiori rispetto al punto di partenza;

a cui si aggiungo due fattori trasversali ad ogni ambito sopra riportato:

- **Landing**, non corretto dimensionamento dell'ambiente target, che a regime impatta sugli SLA di servizio, impattando sulla performance, sui criteri di disponibilità e sull'integrità;
- **Timing**, con un incremento delle tempistiche necessario alla realizzazione del Setup, che impatta sulla disponibilità del servizio.

24.2.1.3 *Migrazione*

In analogia a quanto visto nelle fasi precedenti, anche in quella di Migrazione è condivisa di seguito la stima, che ovviamente dovrà essere contestualizzata a seconda del progetto e della singola Amministrazione, di come le attività di mitigazione previste impattino sui rischi relativi a Disponibilità, Integrità e Performance.

Tabella 18 Valutazione impatti Migrazione

| | Disponibilità | Integrità | Performance |
|---|---|---|---|
| Team Crossfunzionale | ● | ● | ● |
| Iteratività e Incrementalità | ● | ◑ | ◑ |
| Collaborazione con gli Stakeholder dell'Amministrazione | ● | ● | ● |
| Continuos Improvement and Lesson Learned | ● | ◕ | ◕ |
| Standard Documentale | ● | ● | ● |

Oltre ai tre rischi menzionati, gli altri rischi più comuni in tale fase sono legati a:

- **Timing**, con un incremento delle tempistiche di esecuzione, legate alla non corretta pianificazione ed esecuzione della migrazione delle wave in precedenza identificate, che impatta sulla disponibilità del servizio;
- **Moving**, che se mal eseguito, impatta sull'integrità dei dati e delle applicazioni.

In linea con quanto raccomandato **dall'AgID nel suo Manuale di Abilitazione al Cloud**, il costituito RTI ha definito una specifica metodologia, finalizzata a minimizzare i rischi della fase di migrazione, incentrata sui seguenti pillar:

1. **Adozione** di un team di progetto cross-funzionale: il team includerà tutte le competenze necessarie per poter eseguire le attività relative alla migrazione. Tale team cross-funzionale non comprenderà solo competenze tecniche ma anche competenze normative, di processo, di

comunicazione o, in senso più generale, le hard skill e i soft skill capaci di supportare al meglio la transizione al Cloud minimizzando i rischi dovuti a gap conoscitivi;

2. **Iteratività e incrementalità**: sempre in ottica di riduzione del rischio, le attività di migrazione dovranno essere iterative ed incrementali rispetto al set di wave definito nella fase di Analisi/Discovery;
3. **Collaborazione** con gli Stakeholder dell'Amministrazione: il modello di condivisione adottato dal team di migrazione prevede la validazione dei risultati al termine di ogni iterazione, in modo da identificare il prima possibile elementi che richiedano correzioni o variazioni e discutere le criticità emerse che condizionano il raggiungimento dei risultati attesi, fino a ridefinire gli obiettivi se necessario;
4. **Miglioramento Continuo**: al fine di implementare la pratica del miglioramento continuo, il costituito RTI, oltre all'adozione della pratica della retrospettiva, derivata dalla metodologia Agile, nell'ambito del progetto realizzerà un repository delle lesson learned associate alle wave/iterazioni;
5. **Standard Documentale**: i migration set raccolti nelle fasi precedenti, per minimizzare i rischi di Timing e di Moving, saranno raccolti in un detailed plan, che andrà ad indirizzare correttamente tutte le esigenze, i vincoli infrastrutturali ed applicativi emersi, nonché i requisiti di business che si sono evidenziati.

#### 24.2.1.4 *Collaudo*




In analogia a quanto visto nelle fasi precedenti, anche in quella di Collaudo è condivisa di seguito la stima, che ovviamente dovrà essere contestualizzata a seconda del progetto e della singola Amministrazione, di come le attività di mitigation previste impattino sui rischi relativi a Disponibilità, Integrità e Performance.

Un ruolo fondamentale, nel processo di mitigazioni dei rischi, è svolto dalla fase di collaudo, allo scopo di identificare e correggere le potenziali criticità che potrebbero impattare pesantemente sul percorso di Cloud Trasformation intrapreso dall'Amministrazione, con particolare focus sui rischi relativi alla disponibilità, all'integrità e alle performance, in linea con quanto previsto dall'AgID nelle linee guida contenute nel suo Manuale di Abilitazione al Cloud.

Tabella 19 Valutazione impatti Collaudo

| | Disponibilità | Integrità | Performance |
|---|---|---|---|
| Definizione Strategia | ● | ● | ● |
| Pianificazione | ● | ● | ● |
| Progettazione | ● | ● | ● |
| Esecuzione | ● | ● | ● |
| Test di Performance | ● | ● | ● |
| Test di Disponibilità | ● | ● | ● |
| Test di Integrità | ● | ● | ● |
| Riduzione dei Rischi | ● | ● | ● |
| Test di Funzionalità | ● | ● | ● |

A tal proposito, il costituito RTI adotta, in ottica di minimizzazione dei rischi connessi alla migrazione al Cloud una strategia basata su due distinti livelli operativi:

- Il collaudo a livello di singola wave, che, applicando il paradigma DevOps, come indicato dall'AgID, sarà integrato con il processo di migrazione e sarà eseguito per validare il singolo step iterativo, come evidenziato nei paragrafi precedenti;
- Il collaudo globale della piattaforma, che avverrà al termine della migrazione di tutte le wave.

Sia a livello di wave, sia a livello globale, il costituito RTI ha definito una metodologia che, nelle varie fasi, prevederà un processo integrato in cui:

- Si percorrono, ove necessario iterativamente, tutti i processi elementari relativi ai diversi livelli di test (unitario, di integrazione, di sistema);
- Per ognuno di questi processi elementari si disegna la strutturazione delle attività per fasi (pianificazione, progettazione, esecuzione);
- Sono individuati gli opportuni tipi di test, cioè i raggruppamenti logici orientati alla verifica di una specifica categoria di attributi (funzionali o di equivalenza funzionale, prestazionali, usabilità, etc.) con particolare attenzione ai criteri di integrità, affidabilità e performance.

Il collaudo, in ottica di minimizzare il rischio per l'Amministrazione, sarà relativo ai vari livelli di "aggregazione" in cui un sistema a partire dalle sue unità elementari, deve essere verificato.

Il team di migrazione procederà quindi secondo le seguenti fasi, in cui saranno coinvolti gli opportuni stakeholder dell'Amministrazione:

- definizione della strategia: finalizzata alla definizione del tailoring dei test stabilendone gli obiettivi e procedure per la gestione di eventuali anomalie;
- pianificazione: per la definizione degli effort, degli skill necessari e delle tempistiche;
- progettazione: in questa fase vengono stabiliti in dettaglio i test da eseguire a partire dall'importanza e criticità dei requisiti da verificare;
- esecuzione: è la fase in cui i test vengono eseguiti compilando la documentazione relativa ai risultati ottenuti (Test Report e Test Back log).

All'interno della fase di Esecuzione saranno molto importanti i test di Performance, di Integrità, di Disponibilità e di Funzionalità.

24.2.1.5 *Test di Performance*

Tali test, a titolo esemplificativo, saranno riconducibili alle seguenti tipologie

- **Carico,** per verificare le prestazioni dell'infrastruttura per un determinato carico di utilizzo ed in un determinato periodo di tempo. Ad esempio: verifica dei livelli di memoria raggiunti con un carico di 1000 utenti simultanei per 5 minuti;
- **Stress,** per verificare qual è la capacità massima dell'infrastruttura aumentando progressivamente il carico di utilizzo su di essa fino al raggiungimento del limite massimo;
- **Picco,** per verificare come reagisce l'infrastruttura a carichi molto variabili, abbassando o alzando di molto il carico in un determinato range di tempo;
- **Connettività,** per verificare tramite test automatici e manuali la latenza dell'applicativo migrato rispetto a quello on-premise.

Nel processo di validazione delle prestazioni vanno considerati i seguenti passi:

1. Identificazione dei livelli di prestazioni desiderati per metriche come ad esempio:
    a. tempi di risposta;
    b. latenza;
    c. throughput;
2. Definizione dei tipi di test da attuare e dei dati da utilizzare (piano di test);
3. Configurazione degli strumenti di monitoraggio dei livelli di prestazioni identificati;
4. Esecuzione dei test tramite strumenti appositi;
5. Analisi dei risultati ed eventuale tuning delle risorse assegnate alla wave/piattaforma.

A titolo esemplificativo e non vincolante, raccogliendo le indicazioni dell'AgID sull'utilizzo di prodotti/soluzioni open source, potranno essere utilizzati, per l'esecuzione dei test di performance:

- **Jmeter:** strumento utilizzato per le attività di test di performance (load e stress), le cui funzionalità consentono di registrare e rieseguire automaticamente le transazioni sulle applicazioni attraverso degli script personalizzabili;
- **SoapUI**: consente di testare tutte le funzionalità messe a disposizione per la cooperazione applicativa. Viene utilizzato per ispezionare i Web Services ed invocarli senza scrivere codice client, effettuare test funzionali, di carico e di interoperabilità (WS-I) con differenti piattaforme, fornire supporto agli standard dei Web Services SOAP, HTTP(S) con client authentication (WS-security).

24.2.1.6 *Test di Disponibilità*

La disponibilità si riferisce alla possibilità, per i soggetti autorizzati, di poter accedere alle risorse di cui hanno bisogno per un tempo stabilito ed in modo ininterrotto. Rendere un servizio disponibile significa essenzialmente evitarne l'interruzione e ciò richiede che anche le risorse infrastrutturali da esso sottese siano sempre pronte e disponibili.

Per minimizzare i rischi, in linea con quanto richiesto dal Criterio specificamente in tale ambito, saranno realizzati dei test specifici per i singoli casi d'uso, di cui si riporta nel seguito un esempio per maggior chiarezza:

- **Up e Running** dell'Applicazione;
- **Accessibilità** dell'Applicazione, misurando, ad esempio:
    - Il numero massimo di sessioni di accesso concorrenti supportato;
    - Il max carico supportato;
    - La latenza, il jitter e il numero di pacchetti scartati a seconda delle condizioni operative;
    - **DR/BC** in cui simulando il fail over della piattaforma di produzione e delle relative tempistiche.

24.2.1.7 *Test di Integrità*

L'Integrità individua la capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificate o cancellate

A tal fine, il costituito RTI ha ipotizzato, per minimizzare i rischi, in linea con quanto richiesto dal Criterio, di implementare alcune tipologie di test, a titolo esemplificativo, da contestualizzare a seconda dell'ambiente operativo e delle specifiche esigenze dell'Amministrazione:

- **Completezza,** finalizzati a verificare che tutti gli oggetti rilevanti a livello business che si vogliono migrare siano stati effettivamente migrati con successo;
- **Appearance,** finalizzati a ridurre il rischio di inconsistenza dei dati pre e post migrazione;
- **Sicurezza** informatica.

I test di completezza si basano sul concetto di Unità di Migrazione (Unit of Migration, UoM), ovvero l'identificazione di ogni entità rilevante a livello di business che può tradursi in una o più strutture nella base dati (ad es. tabelle), che saranno identificati in collaborazione con gli Stakeholder dell'Amministrazione**.** In particolare, tali test saranno ricondotti a due macrocategorie:

- **Riconciliazione,** per verificare che il numero di entità UoM nel sistema sorgente sia il medesimo nel sistema di destinazione;
- **Validazione,** per verificare che la migrazione non abbia alterato aspetti fondamentali dell'UoM.

Nel testare l'Appearance, sarà verificata a campione, con il supporto degli Stakeholder dell'Amministrazione, la consistenza tra un set di dati presente nella piattaforma on site e quella migrata in cloud. Riguardo alla Sicurezza, si ricorda come piattaforma Cloud e servizi erogati saranno qualificati secondo quanto richiesto negli **Allegati alla Delibera 307 dell'ACN,** con particolare focus su quanto richiesto in ambito sicurezza e risk management.

#### 24.2.1.8 *Test di Funzionalità*

La validazione delle funzionalità punta, attraverso test funzionali, a identificare la presenza o meno di questa tipologia di errori, in modo da minimizzare il relativo rischio e potere provvedere alla sua correzione. La lista delle funzionalità desiderate è testata attraverso la verifica di input e di output corrispondenti, senza porre l'attenzione su come i dati vengano processati. I test simulano l'effettivo utilizzo del sistema dal punto di vista di un utilizzatore e possono essere effettuati sia manualmente, attraverso operatori che eseguono i cosiddetti test case, che automaticamente attraverso l'utilizzo di tool specifici che simulano l'operato di un essere umano.

### 24.2.2 Misure di mitigazione adottate nella fase di Post Migrazione

In analogia a quanto visto nelle fasi precedenti, anche in quella di Post Migrazione è condivisa di seguito la stima, che ovviamente dovrà essere contestualizzata a seconda del progetto e della singola Amministrazione, di come le attività di mitigazione previste impattino sui rischi relativi a Disponibilità, Integrità e Performance:

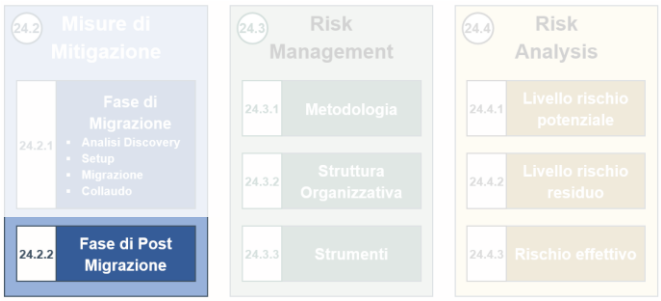



**Figura 56 Focus fase di Post Migrazione**

*Tabella 20 Valutazione impatti Post Migrazione*

| | Disponibilità | Integrità | Performance |
|---|---|---|---|
| Source Shutdown | ● | ● | ● |
| Consolidamento Knowledge | ● | ● | ● |

Durante la fase di Post Migrazione vengono effettuate tutte quelle attività in conclusione alla fase di migrazione che portano allo spegnimento delle risorse, il loro decommissioning e ad un eventuale handover verso la fase di Gestione e Monitoraggio. Inoltre, verranno svolte delle attività di consolidamento e condivisione della Knowledge acquista, al fine di minimizzare i rischi in progetti analoghi.

#### 24.2.2.1 *Source shutdown*

Per un periodo di tempo (detto *periodo di coesistenza*) concordato con l'Amministrazione, l'ambiente di partenza e quello migrato sono entrambi attivi. In tale fase, allo scopo di minimizzare i rischi legati all'hand-over in esercizio della piattaforma, saranno effettuate le seguenti azioni, in collaborazione con gli Stakeholder dell'Amministrazione:

1. Validazione finale dell'attività di migrazione;
2. Eventuale rollback in presenza di issue che implicano il No-Go alla messa in esercizio della piattaforma migrata in Cloud;
3. In linea con quanto previsto dalle linee guida AgID, sarà effettuata una riunione di retrospettiva finalizzata alla misurazione dei KPI di progetto, identificati nella riunione di Start-up, allo scopo

di identificare i risultati/benefici derivati dal processo di migrazione e le eventuali aree di miglioramento;

4. Individuazione e valutazione di eventuali interventi di improvement e fine tuning.

Al termine del periodo di coesistenza la piattaforma di origine potrà essere spenta. Il team di migrazione fornirà all'Amministrazione tutte le informazioni utili per questo scopo, supportandola, in ottica di minimizzazione dei rischi, nella definizione di uno specifico e graduale piano di decommissioning.

In una fase finale verrà effettuato il passaggio di informazioni verso il gruppo che si occuperà della Gestione e del Monitoraggio dell'ambiente migrato attraverso la condivisione delle seguenti informazioni:

- Schemi applicativi;
- Runbook, incluse tutte le specifiche infrastrutturali;
- Documentazione di procedure di gestione (start/stop servizi, manuali utenti etc.);
- Lista di eventuali policy applicate.

24.2.2.2 *Condivisione e consolidamento della Knowledge Acquisita nella Migrazione*

In linea con questo richiesto dall'AgID nelle sue linee guida, il team di progetto del costituito RTI che supporterà l'Amministrazione nel processo di migrazione al Cloud, fungerà da aggregatore di conoscenza impegnato sia nel ruolo di advisor per la stessa, che nella raccolta di know-how ed esperienze di migrazione da condividere con l'unità di controllo e da rendere poi disponibili per le altre Amministrazioni.

A tal proposito il costituito RTI provvederà, a fine progetto a:

- Fornire agli Stakeholder dell'Amministrazione un Feedback Loops formalizzato, che evidenzierà le problematiche emerse e le soluzioni adottate durante le varie fasi del processo, in modo da facilitare l'analisi e la gestione dei rischi in caso di analoghi progetti futuri;
- Allo stesso scopo, consoliderà la Knowledge Base interna, raccogliendo e aggregando le informazioni in termini di manuali operativi, di standardizzazione della documentazione e di disegno di procedure e di processi;
- Supporterà l'Amministrazione, secondo quanto richiesto dall'AgID, nella condivisione della sua esperienza di migrazione nelle Community:
    - **DevOps Italia**, la comunità DevOps per il Cloud delle PA;

- **Forum Italia,** dedicata al tuning dei Cloud Enablement Kit e delle Linee Guida emesse dall'AgID.

## 24.3 Risk Management

### 24.3.1 Metodologia

L'analisi dei rischi connessi alla migrazione è un'attività che viene svolta durante tutte le fasi del progetto, ovvero: 1) Analisi/Discovery, 2) Setup, 3) Migrazione, 4) Collaudo.




**Figura 57 Focus Metodologia**




**Figura 58 Processo di Risk Management**

Il processo di Risk Management, descritto in *Figura 58*, è composto da una serie di attività iterative volte all'identificazione, alla gestione e al controllo degli elementi critici individuati. La gestione degli elementi di rischio prevede la messa in opera da parte del team di governance di tutte le azioni necessarie per mitigare gli impatti degli stessi. Tale processo si articola nelle seguenti fasi:

- **Fase 1. Identificazione dei rischi**: durante questa fase viene effettuato un esame dei cosiddetti "known issues", cioè rischi identificati e già mitigati in precedenza, e degli "unknown issues", ovvero criticità emerse durante l'esecuzione delle attività e non ancora codificati;
- **Fase 2. Analisi dei rischi**: ha l'obiettivo di valutare il livello di esposizione delle attività ad un determinato rischio, denominato Rischio Inerente. La valutazione identificherà la probabilità di accadimento dell'evento e il suo impatto sui benefici e/o sul servizio erogato dall'Amministrazione ai suoi utenti interni ed esterni. In funzione di tali input sarà valutato il livello di esposizione del rischio;
- **Fase 3. Gestione e mitigazione**: la definizione delle tecniche di mitigazione del rischio prevede l'identificazione di un piano d'azione per eliminare o ridurre la probabilità che si verifichi un evento rischioso. Il risultato di questa attività è la stesura di un Piano di Mitigazione del Rischio (PMR);
- **Fase 4. Monitoraggio e controllo**: una volta identificate le azioni di risposta ai rischi secondo quanto definito nel Contingency Plan, il Risk Manager (descritto nel paragrafo successivo) attua le azioni previste nel Risk Register, monitora le criticità e gli indicatori di rischio e predispone il riesame del Risk Register, aggiornato in funzione dei risultati ottenuti.
- **Fase 5. Reporting**: è trasversale alle fasi precedenti e prevede la produzione di report sullo stato di avanzamento delle attività con il riferimento ai rischi mitigati, evitati, variati o dei nuovi che si sono riscontrati durante l'esecuzione del piano e dell'aggiornamento del Risk Register.

Nella seguente tabella è evidenziata la documentazione di Input e Output per ogni fase del processo di Risk Management, che sarà descritta nei sottoparagrafi successivi.

Tabella 21 Documentazione per fase di processo Risk Management

| Fasi | Input | Output |
|---|---|---|
| **Identificazione dei Rischi** | • Lista Know Issue<br>• Lista UnKnow Issue | • Lista Potenziali Minacce alle attività di Migrazione |
| **Analisi Dei Rischi** | • Probabilità Accadimento<br>• Impatto Accadimento | • Valutazione Rischio Inerente<br>• Risk Register |
| **Gestione e Mitigazione** | • Risk Register | • Piano di Mitigazione del Rischio<br>• Contingency Plan |

| Fasi | Input | Output |
|---|---|---|
| **Monitoraggio e Controllo** | • Risk Register | • Update Risk Register |
| **Reporting** | • Risk Register<br>• Piano di Mitigazione del Rischio<br>• Contingency Plan | • Reportistica<br>• Sintesi Indici Qualità Rischio |

Prima dell'avvio della predisposizione di questa documentazione, il Team di Progetto, nella riunione di Start-Up condividerà con gli Stakeholder dell'Amministrazione il relativo Risk Management Plan.

### 24.3.2 Struttura Organizzativa

Facendo riferimento a quanto già descritto in termini di governance e di flussi di comunicazione in risposta a quanto richiesto nel **Criterio ID 17** e nel **Criterio ID 21**, per gestire e coordinare tale processo il costituito RTI ha previsto, nel Piano di Governance relativo al Portfolio Progetti, la figura del **Risk Manager**, con il compito di governare i rischi della fornitura e coordinare le risorse e gli strumenti di Risk & Issue Management tra cui il Risk & Issue Management Team.

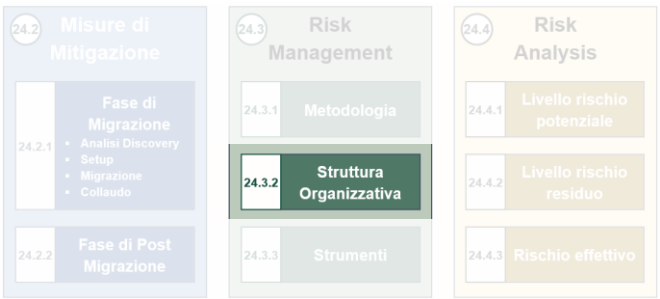



**Figura 59 Focus Struttura Organizzativa**

I compiti di tale team, a livello di singolo progetto, consisteranno in:

- Raccolta di informazioni e valutazione dei rischi;
- Notifica all'Amministrazione dei rischi operativi o di sicurezza, utilizzando i canali preposti;
- Realizzazione di un piano di mitigazione dei rischi in collaborazione con gli stakeholder dell'Amministrazione;
- Monitoraggio degli indici di rischio, loro tracciamento nel Risk Registry e comunicazione all'Amministrazione degli aggiornamenti sulla gestione dei rischi assegnati e dell'avanzamento rispetto ai piani di mitigazione;

- Eventuale coinvolgimento nelle situazioni di rischio immediato e critico del Risk Manager e delle altre figure del Piano di Governance relativo al Portfolio Progetti.

Nei singoli progetti, a seconda della complessità della tipologia di migrazione richiesta dall'Amministrazione, il PMO potrà svolgere anche le funzioni di Risk & Issue Management, rapportandosi comunque con il Risk Manager.

### 24.3.3 Strumenti

Il costituito RTI, facendo riferimento sia alle norme internazionali ISO2 31000:2018 e ISO 31010:2010 e alle best practices contenute sia non PMBOK, sia dal Practice Standard for Project Risk Management editi dal Project Management Institute ha definito una serie di strumenti a supporto del processo di Risk Management, contestualizzato allo specifico contesto dei progetti di migrazione al Cloud, che saranno approfonditi nei sottoparagrafi seguenti. Nella seguente tabella è rappresentata la mappatura tra strumenti proposti dal Costituito ATI, descritti nei sottoparagrafi successivi e le singole fasi del processo di Risk Management

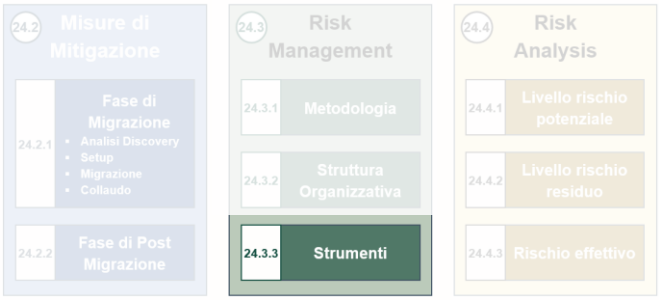



**Figura 60 Focus Strumenti**

Tabella 22 Mappatura strumenti per fasi del processo di Risk Management

| | Risk Management Plan | Risk Register | Mitigation Plan | Contingency Plan | Report | Cruscotti |
|---|---|---|---|---|---|---|
| Identificazione dei rischi | ✓ | | | | | |
| Analisi dei rischi | ✓ | ✓ | | | | |
| Gestione e mitigazione | ✓ | ✓ | ✓ | ✓ | | |
| Monitoraggio e controllo | ✓ | ✓ | | | | ✓ |
| Reporting | ✓ | ✓ | | | ✓ | ✓ |

#### 24.3.3.1 *Risk Management Plan*

Il fulcro del processo di Risk Management è il **Risk Management Plan**, che descrive come la gestione del rischio viene strutturata ed eseguita all'interno del progetto. Il documento conterrà le seguenti informazioni:

- **La metodologia**, ovvero l'approccio, gli strumenti ed i data-sources che possono essere usati per il risk management;
- **I ruoli e le responsabilità,** definendo chi abbia il ruolo principale, chi di supporto e chiarendone le responsabilità nella gestione dei rischi per le singole attività;
- **Timing,** definendo quando e quanto spesso il processo di gestione del rischio sarà eseguito;
- **Le categorie di rischio,** per l'identificazione dei rischi a un livello di dettaglio sufficiente;
- **Le definizioni di probabilità di accadimento e impatto** che verranno usate durante la Risk Analysis;
- **La prima stesura della matrice di probabilità e impatto**;
- **La prima stima della propensione al rischio** da parte degli Stakeholder dell'Amministrazione, che verranno classificati nelle seguenti categorie:
    - **Avverso al rischio**;
    - **Neutrale,** che ricerca l'equilibrio attraverso una attenta analisi delle probabilità ed impatti connessi;
    - **Propenso al Rischio**;
- **Formati dei report,** che definiscono come i risultati dei processi di gestione del rischio saranno documentati, analizzati e comunicati;
- **Tracking** che documenta in che modo le attività di rischio saranno registrate.

24.3.3.2 *Risk Register*

Un elemento fondamentale della gestione del rischio è il Risk Register. Tale documento fornisce un framework che descrive i singoli rischi e come essi vengono trattati. Di seguito, è evidenziato un'ipotesi di template che potrà essere utilizzato dal costituito RTI durante i progetti di migrazione.

| ID | Descrizione | Categoria | Attività | Causa | Probabilità | Impatto | Mitigation | Owner | Status |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

I campi presenti all'interno del Risk Register sono i seguenti:

- **ID** del rischio, per averne una identificazione pratica ed univoca;
- **Descrizione** del rischio;
- **Categoria** a cui appartiene, come ad esempio disponibilità, integrità o performance;
- **Attività** del progetto di migrazione su cui impatta, ad esempio la pianificazione della migrazione;
- **Causa** del rischio;
- **Probabilità di accadimento,** che sarà approfondita nel paragrafo relativo alla Risk Analysis;
- **Impatto,** che sarà approfondito nel paragrafo relativo alla Risk Analysis;
- **Mitigation,** ossia la strategia di risposta al rischio;
- **Owner,** ovvero il responsabile del rischio, che si occupa di gestirlo e ne risponde**;**
- **Status,** se il rischio è gestito, attivo o ancora presente.

#### 24.3.3.3 *Mitigation Plan*

Obiettivo del piano di mitigazione del Rischio è ridurne la probabilità di accadimento o impatto di un evento che possa risultare dannoso per il processo di migrazione. A tale scopo, il costituito RTI ipotizza di proporre agli Stakeholder dell'Amministrazione un documento che, a ogni rischio individuato e analizzato e non accettato, assocerà una specifica scheda contenente le seguenti informazioni:

- **ID**, tratto dal Risk Register;
- **Descrizione del Rischio,** tratta dal Risk Register;
- **Categoria,** tratta dal Risk Register;
- **Attività** impattate nel processo di migrazione, tratte dal Risk Register;
- **Descrizione dettagliata delle relative azioni di mitigazione,** dove, per ogni singola attività, saranno evidenziate:
    - **Pianificazione e tempistiche** di implementazione;
    - **Effort e risorse** impiegate;
    - **Ownership** distribuite tra team di progettazione e Stakehoder dell'Amministrazione;
    - **Vincoli e dipendenze da altre azioni,** che devono essere rispettate affinché l'azione di mitigazione sia attuata.

#### 24.3.3.4 *Contingency Plan*

Il piano di contingency si riferisce alla fase di post-accettazione e post-mitigazione di un rischio, ovvero una volta che il rischio si è verificato. Il loro scopo è quello di permettere al progetto di migrazione di tornare al suo normale svolgimento il più velocemente possibile dopo il verificarsi di un evento

imprevisto. La mitigazione di un rischio, al contrario di un contingency plan, si occupa del rischio prima che esso si manifesti e mira a ridurne la sua probabilità di accadimento o il suo impatto.

Allo scopo di pianificare e gestire al meglio la risposta al verificarsi di un rischio, il costituito RTI ipotizza di proporre agli Stakeholder dell'Amministrazione un documento che a ogni rischio assocerà una specifica scheda contenente le seguenti informazioni:

- **ID,** tratto dal Risk Register;
- **Descrizione del Rischio**, tratta dal Risk Register;
- **Categoria**, tratta dal Risk Register;
- **Attività** impattate nel processo di migrazione, tratte dal Risk Register;
- **Tipologia,** distinguendo tra rischio mitigato e accettato;
- **Trigger,** l'insieme di condizioni che determinano l'attivarsi del processo di contingency;
- **Risorse da proteggere;**
- **Descrizione delle Attività** necessarie per il ripristino delle condizioni normali di migrazione, in cui saranno evidenziate:
    - **Pianificazione e tempistiche** di implementazione;
    - **Effort e risorse impiegate;**
    - **Ownership** distribuite tra team di progettazione e Stakehoder dell'Amministrazione;
    - **Vincoli e dipendenze da altre azioni**, che devono essere rispettate affinché l'azione di mitigazione sia attuata;
- **Condizioni** che debbono essere verificate affinché il processo di contingency si possa considerare concluso e si possa tornare alla normale operatività del processo di migrazione.

#### 24.3.3.5 *Report*

Il reporting nell'ambito del Risk Management ha una doppia funzione: se nel breve periodo migliora la comunicazione all'interno del progetto di migrazione, nel lungo periodo invece crea dei precedenti storici che è possibile utilizzare per ottenere una previsione più accurata di rischi già affrontati in progetti simili.

All'interno dei report sono incluse le seguenti informazioni:

- **ID,** tratto dal Risk Register;
- **Descrizione del Rischio**, tratta dal Risk Register;
- **Categoria,** tratta dal Risk Register;
- **Attività** impattate nel processo di migrazione, tratte dal Risk Register;
- **Sintesi delle azioni di mitigazione** andate a buon fine;

- **Verificarsi dell'evento rischioso**, dettagliando data e durata;
- **Eventuale attivazione** del Contingency Plan;
- **Eventuale rimodulazione** del livello di priorità del rischio.

Al termine della fase di reporting sarà redatto e condiviso con gli Stakeholder dell'Amministrazione un rapporto di sintesi della "qualità del rischio" con indicazione del numero totale di rischi identificati, la percentuale di quelli mitigati con successo e l'impatto su obiettivi, costi e pianificazioni.

24.3.3.6 *Cruscotti*

Facendo riferimento a quanto già descritto nel **Criterio ID 21**, il costituito RTI prevede l'utilizzo di una serie di strumenti dedicati, erogati tramite il Portale della Fornitura, atti a generare valore aggiunto per l'Amministrazione che usufruisce del servizio di migrazione. Il processo di Risk Management sarà monitorato tramite i seguenti strumenti:

- **Issue Log**, dove vengono aggregate tutte le issue che emergono durante le attività di migrazione, approfondito nel criterio precedente**;**
- **Sistema di Monitoraggio dei KPI,** composto da una serie di dashboard e cruscotti, attraverso cui sarà possibile visualizzare, per ciascuna migrazione, un'alberatura a più livelli, partendo dai KPI di aggregazione e consentendo agevolmente il drill down fino al singolo indicatore di impatto o di risultato.

Nella seguente tabella viene descritta la mappatura tra gli strumenti di risk management, che fungeranno da fonti dati e gli strumenti di monitoraggio della migrazione descritti nella risposta al criterio ID 21.

Tabella 23 Mappatura degli strumenti di Risk Management

| | Master Plan | Planner Risorse | Monitoraggio e Controllo del progetto | KPI Monitoring Dashboard | Piano di Change Management | Report di Change Management |
|---|---|---|---|---|---|---|
| **Risk Management** | ✓ | | ✓ | | | |
| **Risk Register** | | | ✓ | | | |
| **Mitigation Plan** | ✓ | ✓ | ✓ | | ✓ | |
| **Contingency Plan** | ✓ | ✓ | ✓ | | ✓ | |
| **Report** | | | | ✓ | | ✓ |

## 24.4 Risk analysis

Nei prossimi paragrafi si descrive la metodologia relativa all'identificazione della probabilità di impatto, all'esposizione ed al calcolo del rischio specifico associato alle singole attività di migrazione.

### 24.4.1 Livello rischio potenziale

Il primo step relativo alla risk analysis è legato alla stima del valore potenziale del servizio da migrare, secondo la seguente classificazione già condivisa nel Criterio ID 20:

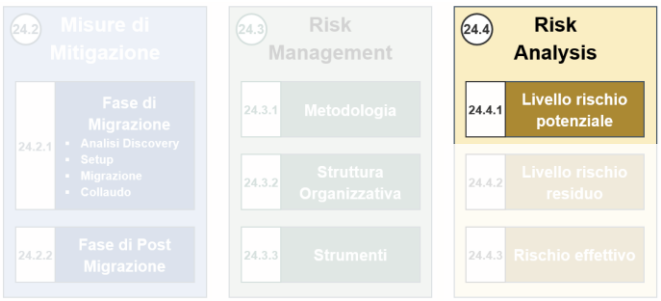



**Figura 61 Focus Livello rischio potenziale**

- **Alto**: la componente è fondamentale per la fornitura del servizio;
- **Medio**: la componente è necessaria per la fornitura del servizio;
- **Basso**: la componente è secondaria per la fornitura del servizio.

A seguito della stima di tale valore, saranno compilate delle specifiche Risk Matrix. La combinazione di una specifica vulnerabilità e della relativa minaccia o evento dannoso, associata a servizio, costituisce il rischio. Al fine di darne una valutazione, si definisce il parametro Livello di Esposizione, consistente nel prodotto tra la Probabilità di Accadimento di un evento dannoso e il suo Impatto sul servizio. La Probabilità di Accadimento di un evento dannoso sarà valutata secondo i criteri esposti nella tabella riportata nel seguito.

Tabella 24 Criteri per valutazione probabilità accadimento

| Livello | Probabilità |
|---|---|
| 1 | Improbabile |
| 2 | Remoto |
| 3 | Possibile |
| 4 | Probabile |
| 5 | Quasi certo |

Stimata la Probabilità di Accadimento, per ogni evento dannoso sarà valutato l'impatto secondo i seguenti valori:

1. Insignificante;
2. Minore;
3. Moderato;
4. Maggiore;
5. Catastrofico.

Per la stima degli impatti, risulteranno presi in considerazione i seguenti elementi:

1. **Integrità**, la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali (involontarie) oppure effettuate volontariamente da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione ex novo di dati ed informazioni;
2. **Disponibilità**, protezione dei dati e delle informazioni nella garanzia di accesso, usabilità e confidenzialità dei dati;
3. **Performance** dei sistemi e delle applicazioni.

### 24.4.2 Livello rischio residuo

Valutati sia la Probabilità di Accadimento, sia l'Impatto, si calcolerà per ogni evento dannoso il parametro "Livello di Esposizione al Rischio", secondo la seguente formula:

**Livello di Esposizione = (Probabilità di Accadimento) X (Impatto Evento Dannoso)**

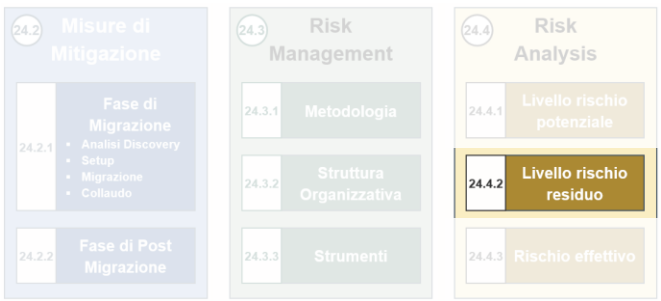



**Figura 62 Focus Livello rischio residuo**

Valutato il Livello di Esposizione per ogni possibile evento dannoso che potrebbe impattare sulla migrazione del servizio, si provvederà alla sua classificazione secondo il criterio evidenziato nella seguente matrice:

Tabella 25 Matrice Livello di Esposizione

| | | Impatto Evento Dannoso | | | | |
|---|---|---|---|---|---|---|
| | | Insignificante | Minore | Moderato | Maggiore | Catastrofico |
| Probabilità di Avvenimento | Quasi certo | Medio | Medio | Alto | Alto | Alto |
| | Probabile | Medio | Medio | Medio | Alto | Alto |
| | Possibile | Basso | Medio | Medio | Medio | Alto |
| | Remoto | Basso | Basso | Medio | Medio | Medio |
| | Improbabile | Basso | Basso | Basso | Medio | Medio |

Tale metodologia di calcolo del livello di esposizione, sarà utilizzata nel seguente processo di Risk Analysis, che si svolgerà in tre fasi distinte:

1. **Fase A:** sarà valutato il livello di esposizione al rischio potenziale delle attività di Migrazione, nel caso non siano adottate misure di mitigazione**,** secondo la metodologia descritta in precedenza;
2. **Fase B:** sarà valutato il livello di esposizione al rischio residuo delle attività di Migrazione, reiterando la precedente analisi, nell'ipotesi che durante la migrazione sia adottato un set di misure "Standard" di mitigazione. Il valore di livello di esposizione sarà calcolato in funzione delle nuove Probabilità di Accadimento e dei nuovi Impatti Stimati;
3. **Fase C:** sarà valutato, in funzione del livello di esposizione al rischio residuo e del valore percepito del servizio erogato dall'Amministrazione a utenti esterni ed interni, il livello di Rischio Effettivo secondo la classificazione indicata nella tabella successiva e la necessità di implementare ulteriori misure di mitigazione.

Tabella 26 Matrice Livello di Esposizione Rischio Residuo

| | | Livello di Esposizione Rischio Residuo | | |
|---|---|---|---|---|
| | | Basso | Medio | Alto |
| Valore Percepito Servizio | Alto | Rischio medio | Rischio alto | Rischio molto alto |
| | Medio | Rischio basso | Rischio medio | Rischio alto |
| | Basso | Rischio basso | Rischio basso | Rischio medio |

Di conseguenza, le attività di migrazione potranno essere classificate in funzione del rischio effettivo nelle seguenti categorie:

- **Rischio molto alto**, in cui l'implementazione di ulteriori misure di mitigazione è necessaria per ridurre ulteriormente il rischio;
- **Rischio alto**, in cui l'implementazione di ulteriori misure di mitigazione è fortemente raccomandata per limitare il rischio;
- **Rischio medio**, in cui l'implementazione di ulteriori misure di mitigazione dovrebbe essere valutata caso per caso;
- **Rischio basso**, in cui l'implementazione di misure di mitigazione può migliorare quelle condivise con gli Stakeholder nella fase di valutazione del livello di esposizione al rischio residuo.

### 24.4.3 Rischio effettivo

A seguito di tale analisi, il costituito RTI provvederà al Trattamento del rischio effettivo, valutando, per ognuna delle attività di migrazione, la necessità di implementare una delle seguenti opzioni:

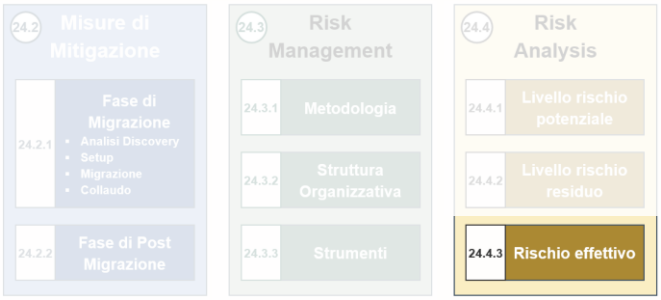



**Figura 63 Focus Rischio effettivo**

- **Riduzione del rischio (impatto)**: il livello di rischio deve essere ridotto attraverso una selezione di controlli, in modo che il rischio effettivo possa essere rivalutato come accettabile;
- **Accettazione del rischio**: la decisione di conservazione del rischio senza intraprendere ulteriori azioni di mitigazione deve essere presa a seconda della valutazione del rischio stesso;
- **Trasferimento del rischio**: il rischio deve essere trasferito ad una terza parte che sia in grado di gestirlo più efficacemente.

# 25 Allegati

**Allegato 01**

# CERTIFICATO DI SISTEMA DI GESTIONE

Certificato n.:
249747-2017-AIS-ITA-ACCREDIA

Data Prima Emissione:
24 novembre 2003

Validità:
20 dicembre 2020 – 19 dicembre 2023

Si certifica che il sistema di gestione di

## LEONARDO S.p.A.

Piazza Montegrappa, 4 - 00195 Roma (RM) - Italy

e i siti come elencati nell'Appendix che accompagna questo certificato

È conforme allo Standard:

**ISO/IEC 27001:2013**

Questa certificazione è valida per il seguente campo applicativo:

**Erogazione dei servizi di Secure Cloud Computing, con l'utilizzo delle linee guida ISO/IEC 27017:2015, 27018:2019 e 27701:2019, dalle aree di Data Center e Service Control Room, relativi a: Servizi Platform as a Virtualizzazione dei servizi di computing, storage, networking ed Infrastructure as a service (IaaS); Servizi Platform as a Service (PaaS); Software as a Service (SaaS); Software Defined Data Center (SDDC) Hosting, Application Hosting di sistemi ERP; Disaster Recovery e Business Continuity. Erogazione di servizi di Data Center Management e Service Operation comprendenti: NOC (Gestione apparati di rete LAN/WAN e relativi sistemi di Sicurezza); Remote Smart Office; Technical Service Desk, monitoraggio e System Management (gestione server di infrastruttura) H24. Erogazione di servizi di: modellazione progettazione e realizzazione di soluzioni di interoperabilità per i dati; progettazione realizzazione e gestione di soluzioni di cooperazione applicativa e di sicurezza applicativa; realizzazione e Gestione di Portali e siti WEB; gestione di contenuti tramite soluzioni di Content Management (CMS); realizzazione e Gestione di Apps" per dispositivi mobili; Realizzazione e Manutenzione Applicativa; Registration Authority per la gestione di Identità Digitali, Firma Digitale remota e fornitura di Certificati di Firma Digitale**
**In accordo con la Dichiarazione di Applicabilità versione del 22 febbraio 2022**
**(Riferimento al Certificato No. 249744-2017-AIS-ITA-ACCREDIA)**

Luogo e Data:
**Vimercate (MB), 07 marzo 2022**

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 003 A
SGA N° 003 D
SGE N° 007 M
SCR N° 004 F
EMAS N° 009 P
PRD N° 003 B
PRS N° 094 C
SSI N° 002 G

Membro di MLA EA per gli schemi di accreditamento SGQ, SGA, PRD, PRS, ISP, GHG, LAB e LAT, di MLA IAF per gli schemi di accreditamento SGQ, SGA, SSI, FSM e PRD e di MRA ILAC per gli schemi di accreditamento LAB, MED, LAT e ISP

Per l'Organismo di Certificazione:
**DNV - Business Assurance**
**Via Energy Park, 14, - 20871 Vimercate (MB) - Italy**

**Claudia Baroncini**
Management Representative

Certificato n.: 249747-2017-AIS-ITA-ACCREDIA
Luogo e Data: Vimercate (MB), 07 marzo 2022

# Appendice al Certificato

**LEONARDO S.p.A.**

I siti inclusi nel certificato sono i seguenti:

| Nome del sito | Indirizzo del sito | Scopo del Sito |
|---|---|---|
| LEONARDO S.p.A. | Piazza Montegrappa, 4 - 00195 Roma (RM) - Italy | Riferimento al campo applicativo |
| LEONARDO S.p.A. | Via Giacomo Puccini, 2 - 16154 Genova (GE) - Italy | Riferimento al campo applicativo |
| LEONARDO S.p.A. | Viale Aeronautica - 80038 Pomigliano d'Arco (NA) - Italy | Riferimento al campo applicativo |

# Attestato di Partecipazione

**ATTENDANCE CERTIFICATE**

al corso

**FOR THE TRAINING COURSE**

## ISO 29100® Foundation

a

**ATTENDED BY**

## Emanuele Rosa

Il corso si è tenuto a Roma nei giorni 10-11 Marzo 2022,

COURSE HAS BEEN HELD IN ROME FROM MARCH THE 10TH TO MARCH THE 11TH

dalle ore 9:00 alle ore 18:00, per un totale di 16 ore di formazione d'aula.

FROM 9.00 AM TO 6.00 PM FOR A TOTAL OF 16 HOURS

Roma, 11/03/2022

ROME, 11/03/2022

SECURITY SOLUTION CONSULTANTS SRL

PECB

BEYOND RECOGNITION

# Professional Evaluation and Certification Board

hereby attests that

## EMANUELE ROSA

is awarded the title

## PECB Certified Privacy Foundation

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

**Certificate Number:** PIFO1100367-2022-03
**Issue Date:** 2022-03-16

Carolina Cabezas
Compliance Director

# Attestato di Partecipazione

**ATTENDANCE CERTIFICATE**

al corso

**FOR THE TRAINING COURSE**

## ISO 29100® Foundation

a

**ATTENDED BY**

## Federica Gentili

Il corso si è tenuto a Roma nei giorni 10-11 Marzo 2022,

COURSE HAS BEEN HELD IN ROME FROM MARCH THE 10TH TO MARCH THE 11TH

dalle ore 9:00 alle ore 18:00, per un totale di 16 ore di formazione d'aula.

FROM 9.00 AM TO 6.00 PM FOR A TOTAL OF 16 HOURS

Roma, 11/03/2022

ROME, 11/03/2022

SECURITY SOLUTION CONSULTANTS SRL

PECB

BEYOND RECOGNITION

# Professional Evaluation and Certification Board

hereby attests that

## FEDERICA GENTILI

is awarded the title

## PECB Certified Privacy Foundation

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

**Certificate Number:** PIFO1100363-2022-03
**Issue Date:** 2022-03-16

Carolina Cabezas
Compliance Director

# Attestato di Partecipazione

**ATTENDANCE CERTIFICATE**

al corso

**FOR THE TRAINING COURSE**

## ISO 29100® Foundation

a

**ATTENDED BY**

## Susanna Marianelli

Il corso si è tenuto a Roma nei giorni 10-11 Marzo 2022,

COURSE HAS BEEN HELD IN ROME FROM MARCH THE 10TH TO MARCH THE 11TH

dalle ore 9:00 alle ore 18:00, per un totale di 16 ore di formazione d'aula.

FROM 9.00 AM TO 6.00 PM FOR A TOTAL OF 16 HOURS

Roma, 11/03/2022

ROME, 11/03/2022

SECURITY SOLUTION CONSULTANTS SRL

PECB

BEYOND RECOGNITION

# Professional Evaluation and Certification Board

hereby attests that

## Susanna Marianelli

is awarded the title

## PECB Certified Privacy Foundation

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

**Certificate Number:** PIFO1100368-2022-03
**Issue Date:** 2022-03-16

Carolina Cabezas
Compliance Director

# Attestato di Partecipazione

**ATTENDANCE CERTIFICATE**

al corso

**FOR THE TRAINING COURSE**

## ISO 29100® Foundation

a

**ATTENDED BY**

## Valeria Montesi

Il corso si è tenuto a Roma nei giorni 10-11 Marzo 2022,

COURSE HAS BEEN HELD IN ROME FROM MARCH THE 10TH TO MARCH THE 11TH

dalle ore 9:00 alle ore 18:00, per un totale di 16 ore di formazione d'aula.

FROM 9.00 AM TO 6.00 PM FOR A TOTAL OF 16 HOURS

Roma, 11/03/2022

ROME, 11/03/2022

SECURITY SOLUTION CONSULTANTS SRL

PECB

BEYOND RECOGNITION

# Professional Evaluation and Certification Board

hereby attests that

## valeria Montesi

is awarded the title

## PECB Certified Privacy Foundation

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

**Certificate Number:** PIFO1100364-2022-03
**Issue Date:** 2022-03-16

Carolina Cabezas
Compliance Director

**Allegato 02**

DNV·GL

# CERTIFICATO
# SISTEMA DI GESTIONE

Certificato n.:
CERT-003-2003-AIS-ROM-SINCERT

Data Prima Emissione:
06 ottobre 2003

Validità:
02 dicembre 2020 – 01 dicembre 2023

Si certifica che il sistema di gestione di

## TIM S.p.A.

Sede legale: Via Gaetano Negri, 1 - 20123 Milano (MI) - Italia

e i siti come elencati nell'Appendix che accompagna questo certificato

È conforme ai requisiti della norma per il Sistema di Gestione:

## ISO/IEC 27001:2013

Questa certificazione è valida per il seguente campo applicativo:

**Sicurezza delle Informazioni (IAF 33, 35)**
**Nei specifici perimetri di:**
* **ICT CONTROL ROOM BUSINESS;**
* **DATA CENTER (Noovle S.p.A.);**
* **SOC;**
* **ICT RISK MANAGEMENT;**
* **SISTEMA CLOUD TOSCANA;**
* **PAYROLL.**

**Per i processi ed i servizi e**
**In accordo alla Dichiarazione di Applicabilità riferite nell'APPENDICE al CERTIFICATO**

Luogo e Data:
**Vimercate (MB), 18 marzo 2021**

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 003 A
SGA N° 003 D
SGE N° 007 M
SCR N° 004 F
EMAS N° 009 P
PRD N° 003 B
PRS N° 094 C
SSI N° 002 G

Membro di MLA EA per gli schemi di accreditamento SGQ, SGA, PRD, PRS, ISP, GHG, LAB e LAT, di MLA IAF per gli schemi di accreditamento SGQ, SGA, SSI, FSM e PRD e di MRA ILAC per gli schemi di accreditamento LAB, MED, LAT e ISP

Per l'Organismo di Certificazione:
**DNV GL - Business Assurance**
**Via Energy Park, 14**
**20871 Vimercate (MB) - Italy**

**Zeno Beltrami**
Management Representative

Certificato n.: CERT-003-2003-AIS-ROM-SINCERT
Luogo e Data: Vimercate (MB), 18 marzo 2021

# Appendice al Certificato

**TIM S.p.A.**

I siti inclusi nel certificato sono i seguenti:

| Nome del sito | Indirizzo del sito | Campo applicativo |
|---|---|---|
| **TIM S.p.A.**<br>**ICT CONTROL ROOM BUSINESS**<br>CERTCC1-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Via di Macchia Palocco, 223<br>00125 Roma (RM) – Italia<br><br>Via Oriolo Romano, 257<br>00189 Roma (RM) – Italia<br><br>Via di Tor Pagnotta, 68<br>00143 Roma (RM) – Italia<br><br>Via delle Conce, Snc<br>00154 Roma (RM) – Italia<br><br>Piazzale Mater Ecclesiae, 5<br>70124 Bari (BA) – Italia<br><br>Centro Direzionale, Isola F7 -<br>80143 Napoli (NA) – Italia<br><br>Via Campania, 11<br>74121 Taranto (TA) – Italia<br><br>Via Marco Aurelio, 28<br>20127 Milano (MI) – Italia<br><br>Via Esiodo, 2<br>30173 Venezia (VE) – Italia<br><br>Via Piero Maroncelli, 1<br>40126 Bologna (BO) – Italia<br><br>Via Aldo Manuzio, 13 - 16143<br>Genova (GE) – Italia | Data Center & Cloud Computing Services in modalità IaaS (Infrastructure as a Service) con l'utilizzo della linea guida ISO/IEC 27018:2019 e con l'utilizzo della linea guida ISO/IEC 27017:2015 per i servizi di Self Data Center "vCloud & Hypervisor".<br>Data Center & Cloud Computing Services in modalità SaaS (Software as a Service) con l'utilizzo della linea guida ISO/IEC 27018:2019 e con l'utilizzo della linea guida ISO/IEC 27017:2015 per il servizio "TIM Work".<br>Servizi di ICT Security con l'utilizzo delle linee guida ISO/IEC 27035:2016-1 e ISO/IEC 27035:2016-2.<br>Network Services, Unified Communication & Collaboration Services, Mobile Services.<br>In accordo con la Dichiarazione dell'Applicabilità ver 8 del 30/09/2020 |

Certificato n.: CERT-003-2003-AIS-ROM-SINCERT
Luogo e Data: Vimercate (MB), 18 marzo 2021

| Nome del sito | Indirizzo del sito | Campo applicativo |
|---|---|---|
| **Noovle S.p.A.**<br>**DATA CENTER**<br>CERTCC2-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Via Oriolo Romano, 240<br>00189 Roma (RM) – Italia<br><br>Via Issiglio, 90<br>10141 Torino (TO) – Italia<br><br>Via Fulvio Bracco 39<br>20811 Cesano Maderno (MB)- Italia<br><br>Viale Toscana, 3<br>20089 Rozzano (MI) – Italia<br><br>Via della Centralinista, 3<br>40138 Bologna (BO) – Italia<br><br>Via Settima strada, 22<br>35129 Padova (PD) - Italia<br><br>Viuzzo dei Bruni, 6<br>50133 Firenze (FI) – Italia<br><br>Via Pontina, km 29,1<br>00040 Pomezia (RM) – Italia<br><br>Via di Macchia Palocco, 223/243<br>00125 Roma (RM) – Italia<br><br>Via Oriolo Romano, 257<br>00189 Roma (RM) – Italia<br><br>Via Giuseppe Macaggi, 12<br>16121 Genova (GE) - Italia | Predisposizione, attivazione ed esercizio di infrastrutture, piattaforme e servizi di Information Communications Technology presso i Data Center e Centri Servizi TIM anche in modalità cloud e virtuale, attraverso:<br>* la gestione di facilities e di impianti tecnologici;<br>* la gestione e assurance di infrastrutture, servizi di rete e firewall;<br>* la gestione della sicurezza fisica alle sale sistemi;<br>* la predisposizione e configurazione dei siti e sale sistemi;<br>* l'attivazione ed esercizio di piattaforme e servizi IT;<br>* la conduzione dei Sistemi Elaborativi.<br>In accordo con la Dichiarazione dell'Applicabilità ver 1.3 del 16/11/2020 |
| **TIM S.p.A.**<br>**SECURITY OPERATION CENTER**<br>CERTCC3-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Via di Val Cannuta, 182<br>00166 Roma (RM) – Italia<br><br>Viale Stelvio, 15<br>20159 Milano (MI) - Italia | Monitoraggio e gestione degli incidenti di sicurezza ICT con l'utilizzo delle linee guida ISO/IEC 27035:2016-1 e ISO/IEC 27035:2016-2<br>In accordo con la Dichiarazione dell'Applicabilità ver 1.1 del 23/11/2020 |
| **TIM S.p.A.**<br>**ICT RISK MANAGEMENT**<br>CERTCC4-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Via di Macchia Palocco, 223/243<br>00125 Roma (RM) – Italia<br><br>Via Gugliemo Reis Romoli, 274<br>10148 Torino (TO) - Italia | ICT Risk Management per gli asset tecnologici del Gruppo Tim:<br>* ICT Risk Management Master Plan;<br>* Individuazione dei rischi e contromisure;<br>* Monitoraggio del rischio ICT;<br>* Controlli di sicurezza ICT.<br>In accordo con la Dichiarazione dell'Applicabilità ver 1.1 del 05/10/2020 |

Certificato n.: CERT-003-2003-AIS-ROM-SINCERT
Luogo e Data: Vimercate (MB), 18 marzo 2021

| Nome del sito | Indirizzo del sito | Campo applicativo |
|---|---|---|
| **TIM S.p.A.**<br>**SISTEMA CLOUD TOSCANA**<br>CERTCC5-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Viale Alessandro Guidoni, 42<br>50127 Firenze (FI) – Italia<br><br>Via S. Piero a Quaracchi, 250<br>50145 Firenze (FI) – Italia<br><br>Viuzzo dei Bruni, 6<br>50133 Firenze (FI) – Italia<br><br>Via di Macchia Palocco, 223/243<br>00125 Roma (RM) – Italia<br><br>Via Fulvio Bracco 39<br>20811 Cesano Maderno (MB) – Italia | Gestione dell'infrastruttura fisica e informatica del Data Center SCT (Sistema Cloud Toscana);<br>Progettazione e erogazione di servizi cloud computing (IaaS, PaaS e SaaS);<br>Erogazione di servizi di Housing e Hosting, posta elettronica, backup da remoto, disaster recovery;<br>Gestione e monitoraggio dei sistemi e della rete.<br>In accordo con la Dichiarazione dell'Applicabilità ver 1.0 del 09/10/2020 |
| **TIM S.p.A.**<br>**PAYROLL**<br>CERTCC6-003-2003-AIS-ROM-SINCERT | Via Gaetano Negri, 1<br>20123 Milano (MI) – Italia<br><br>Via delle Conce, 12<br>00154 Roma (RM) - Italia | Gestione, governo e controllo del ciclo di payroll<br>In accordo con la Dichiarazione dell'Applicabilità ver 1.9 del 01/09/2020 |

# CERTIFICATO DI SISTEMA DI GESTIONE

Certificato n.:
120835-2012-AIS-ITA-ACCREDIA

Data Prima Emissione:
09 agosto 2012

Validità:
20 dicembre 2020 – 19 dicembre 2023

Si certifica che il sistema di gestione di

## LEONARDO S.p.A.

Piazza Montegrappa, 4 - 00195 Roma (RM) - Italy

e i siti come elencati nell'Appendix che accompagna questo certificato

È conforme allo Standard:

**ISO/IEC 27001:2013**

Questa certificazione è valida per il seguente campo applicativo:

**Gestione della Sicurezza delle informazioni per: progettazione, integrazione, manutenzione installazione e assistenza di sistemi di sicurezza informatica gestita (compresi i servizi di SOC Security Operation Center e CERT Computer Emergency Response Team), servizi di sviluppo, gestione e manutenzione di sistemi informativi; progettazione, conduzione tecnica e operativa, monitoraggio e continuità operativa di Data Center in relazione a servizi di cloud computing di tipo IaaS, PaaS e SaaS, servizi di firma digitale, gestione identità digitali, sicurezza applicativa e perimetrale, servizi professionali di supporto; progettazione, implementazione ed erogazione di servizi di Security Intelligence, servizi di modellazione, progettazione, realizzazione e gestione di soluzioni di interoperabilità per i dati (Linked Data/Open Data/Big Data) e soluzioni di cooperazione applicativa; realizzazione e gestione di portali e siti Web, soluzioni di Content Management, applicazioni per dispositivi mobili finalizzati alla loro fruizione; Servizi di disegno e integrazione di soluzioni IT Progettazione ed erogazione di servizi di consulenza in ambito Security Governance e Privacy.**
**In accordo con la Dichiarazione di Applicabilità versione del 25 febbraio 2022 e mediante l'applicazione della Linea Guida ISO/IEC 27035-1,2:2016**
**(Riferimento al Certificato No. 249744-2017-AIS-ITA-ACCREDIA)**

Luogo e Data:
**Vimercate (MB), 07 marzo 2022**

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 003 A
SGA N° 003 D
SGE N° 007 M
SCR N° 004 F
EMAS N° 009 P
PRD N° 003 B
PRS N° 094 C
SSI N° 002 G

Membro di MLA EA per gli schemi di accreditamento SGQ, SGA, PRD, PRS, ISP, GHG, LAB e LAT, di MLA IAF per gli schemi di accreditamento SGQ, SGA, SSI, FSM e PRD e di MRA ILAC per gli schemi di accreditamento LAB, MED, LAT e ISP

Per l'Organismo di Certificazione:
**DNV - Business Assurance**
**Via Energy Park, 14, - 20871 Vimercate (MB) - Italy**

**Claudia Baroncini**
Management Representative

Certificato n.: 120835-2012-AIS-ITA-ACCREDIA
Luogo e Data: Vimercate (MB), 07 marzo 2022

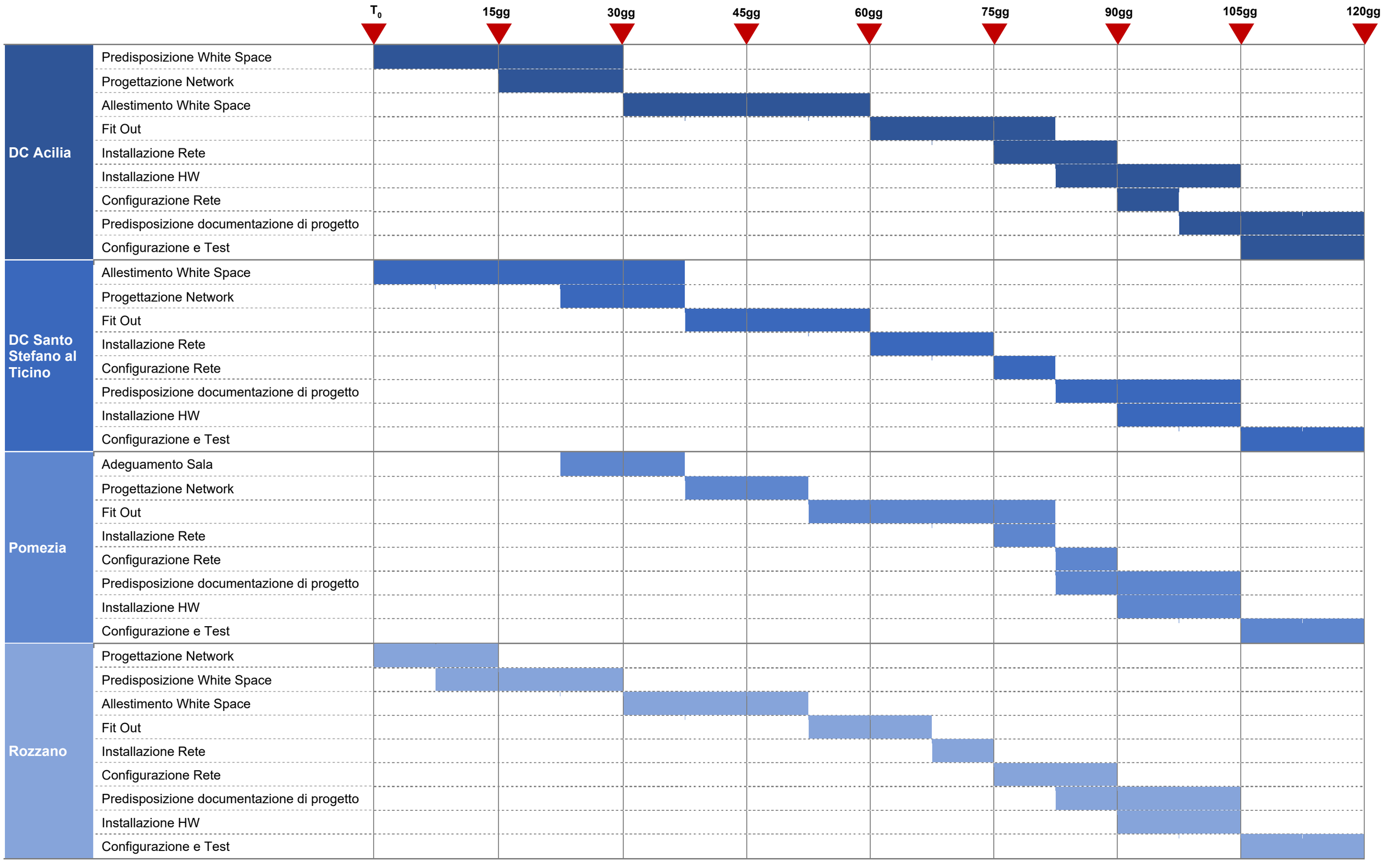
# Appendice al Certificato

**LEONARDO S.p.A.**

I siti inclusi nel certificato sono i seguenti:

| Nome del sito | Indirizzo del sito | Scopo del Sito |
|---|---|---|
| LEONARDO S.p.A. | Piazza Montegrappa, 4 - 00195 Roma (RM) - Italy | Riferimento al campo applicativo |
| LEONARDO S.p.A. | Via Enrico Mattei, 21 - 66100 Chieti (CH) - Italy | Riferimento al campo applicativo |
| LEONARDO S.p.A. | Via Laurentina, 760 - 00143 Roma (RM) - Italy | Riferimento al campo applicativo |

**Allegato 03**


T0
15gg
30gg
45gg
60gg
75gg
90gg
105gg
120gg
DC Acilia
Predisposizione White Space
Progettazione Network
Allestimento White Space
Fit Out
Installazione Rete
Installazione HW
Configurazione Rete
Predisposizione documentazione di progetto
Configurazione e Test
DC Santo Stefano al Ticino
Allestimento White Space
Progettazione Network
Fit Out
Installazione Rete
Configurazione Rete
Predisposizione documentazione di progetto
Installazione HW
Configurazione e Test
Pomezia
Adeguamento Sala
Progettazione Network
Fit Out
Installazione Rete
Configurazione Rete
Predisposizione documentazione di progetto
Installazione HW
Configurazione e Test
Rozzano
Progettazione Network
Predisposizione White Space
Allestimento White Space
Fit Out
Installazione Rete
Configurazione Rete
Predisposizione documentazione di progetto
Installazione HW
Configurazione e Test

**Allegato 04**

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-4533

Si certifica che il Sistema di Gestione della Sicurezza e della Salute sul luogo di lavoro di
*It is hereby certified that the Occupational Health and Safety Management System of*

## TELECOM ITALIA S.P.A.

VIA GAETANO NEGRI, 1 20123 MILANO (MI) ITALIA

nelle seguenti unità operative/ *in the following operational units*

CORSO D'ITALIA 41, 00198 ROMA (RM) ITALIA

E UNITÀ OPERATIVE INDICATE NELLE PAGINE SUCCESSIVE/*AND OPERATIVE UNITS LISTED IN THE NEXT PAGES*

è conforme alla norma / *is in compliance with the standard*

## ISO 45001:2018

per i seguenti campi di attività / *for the following field(s) of activities*

PROGETTAZIONE, REALIZZAZIONE, MANUTENZIONE E GESTIONE DEGLI IMMOBILI DI COMPETENZA DI REAL ESTATE. GESTIONE DELL'AUTOPARCO AZIENDALE

*IAF:31*
*IAF:28*
*IAF:35*

*DESIGN, CONSTRUCTION, MAINTENANCE AND MANAGEMENT OF REAL ESTATE BUILDINGS. MANAGEMENT OF COMPANY CAR FLEET*

La validità del presente certificato è subordinata a sorveglianza periodica annuale / semestrale ed al riesame completo del sistema di gestione con periodicità triennale
*The validity of this certificate is dependent on an annual/six monthly audit and on a complete review, every three years, of the management system*

L'uso e la validità del presente certificato è soggetto al rispetto del documento RINA: Regolamento per la Certificazione dei Sistemi di Gestione della Sicurezza e Salute sul luogo di lavoro
*The use and validity of this certificate are subject to compliance with the RINA document: Rules for the Certification of Occupational Health and Safety Management Systems*

| | | | |
|---|---|---|---|
| Prima emissione *First Issue* | 10.12.2021 | | |
| Data scadenza *Expiry Date* | 09.12.2024 | Data revisione *Revision date* | 10.12.2021 |

Paolo Teramo
Italy Management System Certification Region, Senior Director

**RINA Services S.p.A.**
Via Corsica 12 – 16128 Genova Italy

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Itre unità operative coperte dal sistema di gestione di:**
***Other operational units covered by the management system of:***

## TELECOM ITALIA S.P.A.

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità operative/*Operational units*<br>(Ragione sociale-Indirizzo Sito / *Registered name-Site address)*** |
|---|
| SS 189, snc San Giusippuzzu - 92100 Agrigento AG |
| Via Tripoli, 18 – 15040 Alessandria AL |
| Via Guido Miglioli 24 - 60131 Ancona AN |
| Via Caduti Del Lavoro 40 - 60131 Ancona AN |
| Corso Stamira 46 - 60122 Ancona AN |
| Via Carlo Viola, 65 - 11026 Pont-Saint-Martin AO |
| Via Sardegna 2 – 63037 Ascoli Piceno AP |
| Via Strinella 2 - 67100 L'Aquila AQ |
| Via Petrarca 32/34/36 – 52100 Arezzo AR |
| Via Due Principati 88 - 83100 Avellino AV |
| Via Loquercio 38 – 70131 Bari BA |
| Via Pietro Oreste 20 - 70123 Bari BA |
| Via Napoli 331 - 70123 Bari BA |
| Via De Saussurre, 1 – 24100 Bergamo BG |
| Via T. Tasso 121 – 24100 Bergamo BG |
| Via Duca D'Aosta snc - 82100 Benevento BN |
| Via Della Centralinista 3 - 40138 Bologna BO |
| Piazza VIII Agosto, Via Piero Maroncelli - 40126 Bologna BO |
| Via Goito, 13 – 40100 Bologna BO |
| Via del Pallone 1,3,5 – 40100 Bologna BO |
| Via Francesco Albani 3 - 40129 Bologna BO |
| Via Henri Beyle Stendhal 31 - 40128 Bologna BO |
| Via Cefalonia, 41 - 25124 Brescia BS |

Data revisione
*Revision date* 10.12.2021

SCR N° 003 F

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

| **Unità operative/*Operational units*** **(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)** |
|---|
| Via Resia 188 - 39100 Bolzano BZ |
| Via Calamattia 17 - 09134 Cagliari CA |
| Via Matteo Maria Boiardo 12 - 09128 Cagliari CA |
| Via Conte Rosso 20 - 86100 Campobasso CB |
| Via Galatina Snc - San Clemente - 81100 Caserta CE |
| Via Leone XIII, snc - 93100 Caltanissetta CL |
| Via Giovanni Battista Bongioanni 17 - 12100 Cuneo CN |
| Via Dante Alighieri, snc - 22100 Como CO |
| Via Cadolini 1 – 26100 Cremona CR |
| Via Panebianco 297 - 87100 Cosenza CS |
| Piazza Francesco Crispi - Via Millelli, snc - 87100 Cosenza CS |
| Via Ala, snc - 95123 Catania CT |
| Piazza Università 2 – 95010 Catania CT |
| Via Mons. Domenico Orlando 10/12 - 95126 Catania CT |
| Via dei Gelsomini, snc Contrada San Cono – 88100 Catanzaro CZ |
| Via Monsignor Giovanni Fiorentini 5 - 88100 Catanzaro CZ |
| Via Cairoli 19 - 44100 Ferrara FE |
| Via Benedetto Biagi 8 - 71100 Foggia FG |
| Via Carlo Baffi, 1 ang. Via Candelaro, 34 – 71100 Foggia FG |
| Viale Alessandro Guidoni 40/42 - 50127 Firenze FI |
| Viuzzo dei Bruni, 8 (Via P. Jahier, 6) 50100 Firenze FI |
| Via Valle Fioretta 281 - 03100 Frosinone FR |
| Via Aldo Manuzio 13 -16143 Genova GE |
| Via Bartolomeo Bianco 5 - 16127 Genova GE |
| Via Giuseppe Macaggi 12 - 16121 Genova GE |
| Via Pra 8b - 16157 Genova GE |
| Via Manetti 4 - 58100 Grosseto GR |
| Via Lupiae 50 - 73100 Lecce LE |
| Via Taranto D'Aurio, 68 - 73100 Lecce LE |
| S.S. Monti Lepini 156 - 04100 Latina LT |
| Via Duca Del Mare 35 - 04100 Latina LT |
| Via Molise 19 - 20900 Monza MB |

Data revisione
*Revision date* 10.12.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

| **Unità operative/*Operational units*** **(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)** |
|---|
| Via Carlo Giuliozzi 32 - 62100 Macerata MC |
| Corso Cavour, snc ang. Piazza Fontanta Gennaro - 98122 Messina ME |
| Via Ducezio snc - 98124 Messina ME |
| Via Gaetano Negri 1/Via S.M. Segreta 3 - 20123 Milano MI |
| Via Della Boscaiola 26 - 20159 Milano MI |
| Via Tonale 11 - 20125 Milano MI |
| Via Marco Aurelio 24/26 - 20127 Milano MI |
| Viale Toscana 3/5 - 20089 Rozzano MI |
| Via Magolfa 10 - 20143 Milano MI |
| Via Filippo Corridoni 13-15 - 46100 Mantova MN |
| Via Michele Fusco 28 - 41100 Modena MO |
| Via G. Fortunato, snc – 75100 Matera MT |
| Viale della Costituzione - Isola F5, F6, F7 - 80143 Napoli NA |
| Via della Stadera 66 - 80143 Napoli NA |
| Salita Scudillo 20 - 80131 Napoli NA |
| Viale Giulio Cesare 345 - 28100 Novara NO |
| Piazza Giacomo Matteotti 2/4 - 28100 Novara NO |
| Via Ugo La Malfa 99 - 90147 Palermo PA |
| Via Ugo La Malfa 159 - 90147 Palermo PA |
| Via Plauto 29 - 90148 Palermo PA |
| Via Caduti Sul Lavoro 45 - 29100 Piacenza PC |
| Via 7a Strada 20 - 35122 Padova PD |
| Via Pietro Donà 3/4 - 35129 Padova PD |
| Via Tiburtina Valeria 419 - 65129 Pescara PE |
| Via Monte Viglio, snc - 65124 Pescara PE |
| Via Bardet 34/A - 65126 Pescara PE |
| Via Milano 35/37 – Via Genova 7/9/19/21/2 - 65122 Pescara PE |
| Via Monteripido snc - 06125 Perugia PG |
| S.S. dell'Abetone e del Brennero – Figuretta - 56123 Pisa PI |
| Via Po 7 - 43100 Parma PR |
| Via Nazario Sauro Snc - 85100 Potenza PZ |
| Via Antonio Meucci 17 - 48100 Ravenna RA |

Data revisione
*Revision date* 10.12.2021

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

| **Unità operative/*Operational units*<br>(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)** |
|---|
| Via Reggio Campi 93 - 89126 Reggio Calabria RC |
| Via Paolo Toschi 27 - 42100 Reggio Emilia RE |
| Viale Europa snc - 97100 Ragusa RG |
| Viale Ludovico Canali 10 - 02100 Rieti RI |
| Via Oriolo Romano 240 - 00189 Roma RM |
| Via Di Macchia Palocco 223 - 00125 Roma RM |
| Via Di Val Cannuta 182 - 00166 Roma RM |
| Via Del Pellegrino 155 - C.so Vittorio Emanuele 208 - 00186 Roma RM |
| Via Oriolo Romano 257 - 00189 Roma RM |
| Corso Italia 41 - 00198 Roma RM |
| Via Stazione Tuscolana 104 - 00182 Roma RM |
| Via Santa Maria In Via 6/7/7A/9 - 00187 Roma RM |
| Via Saffi 58/64, Via San Francesco D'Assisi - 00041 Albano Laziale RM |
| Via della Tenutella ang V. S.Antonio in Canepina - Fraz. Cordaro - 00041 Albano Laziale RM |
| Largo Valerio Bacigalupo 9 - 00142 Roma RM |
| Via Sannio 17/23 – 00183 Roma RM |
| Piazza Trento 10 – 00198 Roma RM |
| Via C. Armellini 11/13 – 00153 Roma RM |
| Via degli Estensi, 52-88 - 00164 Roma RM |
| Via Di Tor Pagnotta 68/70 - 00143 Roma RM |
| Via Fiume Bianco 8 - 00144 Roma RM |
| Viale Guglielmo Marconi 264 - 00146 Roma RM |
| Via Bartolomeo Marliano 27 - 00162 Roma RM |
| Via Pineta Sacchetti 229 - 00168 Roma RM |
| Via del Cottolengo, 61 - 00165 Roma RM |
| Via Walter Procaccini 67 - 00173 Roma RM |
| Via Delle Conce 10 - 00154 Roma RM |
| Via Della Cesarina 282 - 00139 Roma RM |
| Via Ernestro Nathan 110 - 00146 Roma RM |
| S.S.148 Pontina Km 29,100 - 00040 Pomezia RM |
| Via Angelo Emo 13F - 00136 Roma RM |
| Via Romania 46 - 47900 Rimini RN |

Data revisione
*Revision date* 10.12.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

| **Unità operative/*Operational units*<br>(Ragione sociale-Indirizzo Sito / *Registered name-Site address)*** |
|---|
| Via Donato Bramante 12 - 47900 Rimini RN |
| Via Raffaele Mauri 201 - 84132 Salerno SA |
| Via Ricasoli 93 - 53100 Siena SI |
| Viale Tica, snc – 96100 Siracusa SR |
| Corso Tardy E Benech 140R - 17100 Savona SV |
| Via Campania 11 - 74121 Taranto TA |
| Via Valentina Zambra 1 - 38100 Trento TN |
| Via Isonzo 112 - 10141 Torino TO |
| Via Vincenzo Lancia 55 - 10141 Torino TO |
| Via Guglielmo Reiss Romoli 274 - 10148 Torino TO |
| Via Montenavale 1 -10015 Ivrea TO |
| Via Montenavale 2/C -10015 Ivrea TO |
| Via Marino Torre, snc - 91100 Trapani TP |
| Via Mentana 43 - 05100 Terni TR |
| Via Carlo Forlanini 39 - 34139 Trieste TS |
| Via Giovanni Pascoli 9 - 34138 Trieste TS |
| Via Sante Zanon 7 - 31100 Treviso TV |
| Via Dei Carlini, snc -33100 Udine UD |
| Viale Luigi Borri 150 – 21100 Varese VA |
| Via Torino 84 – 30172 Venezia VE |
| Via Esiodo 2 – 30173 Venezia VE |
| Piazza Donatori Sangue, snc – 30171 Venezia VE |
| Via Giovanni Battista Quadri 121 – 36100 Vicenza VI |
| Via Giuseppe Belluzzo 12 - 37132 Verona VR |
| Via Igino Garbini, snc - 01100 Viterbo VT |

Data revisione
*Revision date* 10.12.2021

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

SCR N° 003 F

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ

www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* ABMS-105/19

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

SI CERTIFICA CHE IL SISTEMA DI GESTIONE ANTICORRUZIONE DI
*IT IS HEREBY CERTIFIED THAT THE ANTI-BRIBERY MANAGEMENT SYSTEM OF*

## TELECOM ITALIA S.P.A.

VIA GAETANO NEGRI, 1 20123 MILANO (MI) ITALIA

NELLE SEGUENTI UNITÀ OPERATIVE / *IN THE FOLLOWING OPERATIONAL UNITS*
CORSO D'ITALIA 41, 00198 ROMA (RM) ITALIA

E UNITÀ OPERATIVE INDICATE NELLE PAGINE SUCCESSIVE/*AND OPERATIVE UNITS LISTED IN THE NEXT PAGES*
E CANTIERI OPERATIVI/*AND OPERATIONAL YARDS*

È CONFORME ALLA NORMA / *IS IN COMPLIANCE WITH THE STANDARD*

## ISO 37001:2016

PER I SEGUENTI CAMPI DI ATTIVITÀ / *FOR THE FOLLOWING FIELD(S) OF ACTIVITIES*

SERVIZI DI COMUNICAZIONI FISSE, MOBILI E SOLUZIONI ICT OLTRE A SERVIZI A CONTENUTO DIGITALE, GESTIONE DI RETE FISSA PER VOCE E DATI E DI PIATTAFORMA RETE MOBILE DIFFUSE A LIVELLO NAZIONALE

*FIXED AND MOBILE TELECOMMUNICATION SERVICES AND ICT SOLUTIONS IN ADDITION TO DIGITAL CONTENT SERVICES, MANAGEMENT OF A VOICE AND DATA FIXED NETWORK AND A MOBILE NETWORK PLATFORM DISTRIBUTED ON A NATIONAL LEVEL*

La validità del presente certificato è subordinata a sorveglianza periodica annuale / semestrale ed al riesame completo del sistema di gestione con periodicità triennale
*The validity of this certificate is dependent on an annual/six monthly audit and on a complete review, every three years, of the management system*
L'uso e la validità del presente certificato sono soggetti al rispetto del documento RINA: Regolamento per la Certificazione di Sistemi di Gestione Anticorruzione
*The use and validity of this certificate are subject to compliance with the RINA document: Rules for the Certification of Anti-bribery Management Systems*

| | | | |
|---|---|---|---|
| Prima emissione *First Issue* | 14.10.2019 | | |
| Data scadenza *Expiry Date* | 13.10.2022 | Data revisione *Revision date* | 14.10.2019 |

Emanuele Castagno
Executive Vice President
Certification

**RINA Services S.p.A.**
Via Corsica 12 – 16128 Genova Italy

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Altre unità operative coperte dal sistema di gestione di:**
***Other operational units covered by the management system of:***

## TELECOM ITALIA S.P.A.

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 37001:2016

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address)***

| | |
|---|---|
| Via Degli Estensi 88 - 00164 Roma RM | Via Sebastiano Barozzi 58 - 32100 Belluno BL |
| Via Oriolo Romano 240 - 00189 Roma RM | Via Monfalcone 41D - 19123 La Spezia SP |
| Via Di Tor Pagnotta 74 - 00143 Roma RM | Via Montebianco 28 - 05018 Orvieto TR |
| Corso Bramante 20 - 10134 Torino TO | Via Vallesina 34 - 35042 Este PD |
| Via Di Macchia Palocco 223 - 00125 Roma RM | Via S.Rocco Snc - 84036 Sala Consilina SA |
| Via Aurelio Saliceti 2 - 00153 Roma RM | Via Guido Reni 6 - 50065 Pontassieve FI |
| Via Di Val Cannuta 182 - 00166 Roma RM | Largo Botteghelle Snc - 89132 Reggio Calabria RC |
| Via Del Pellegrino 155 - 00186 Roma RM | Via Vittorio Veneto 34 - 17031 Albenga SV |
| Via Oriolo Romano 257 - 00189 Roma RM | Via Ippocrate, snc - 87067 Rossano CS |
| Via Fonte Buono 78 - 00142 Roma RM | Corso Tardy E Benech 138R - 17100 Savona SV |
| Corso D'Italia 41 - 00198 Roma RM | Via Nazario Sauro - 67051 Avezzano AQ |
| Via Parini 6 - 20121 Milano MI | Via Dante Alighieri snc - 06012 Città di Castello PG |
| Via Marco Aurelio 26 - 20127 Milano MI | Via Ludovico Ariosto snc - 06034 Foligno PG |
| Via Della Vignaccia 167 - 00163 Roma RM | Aurelia Antica - 58015 Orbetello GR |
| Via Roberto Ardigò 13/A - 10134 Torino TO | Via Carlo Marx 9 - 15011 Acqui Terme AL |
| Via Stazione Tuscolana 104 - 00182 Roma RM | Via Danna 4 - 12100 Savigliano CN |
| Via Gaetano Negri 1 - 20123 Milano MI | Via Fossati 2 - 25087 Salò BS |
| Via Della Centralinista 3 - 40138 Bologna BO | Viuzzo De' Bruni 8 - 50133 Firenze FI |
| Via Degli Agrostemmi 30 - 00134 Roma RM | Via Cesare Beccaria, Ang. Via Cibali - 95123 Catania CT |
| Via Pietro Crespi 1 - 20127 Milano MI | Via Sparano 160 - 70121 Bari BA |
| Via Santa Maria In Via 9 - 00187 Roma RM | Via Manfredo Da Passano 30 - 19121 La Spezia SP |
| Via Valle Dei Fontanili Snc - 00168 Roma RM | Via Sanguinetti 9 - 17014 Cairo Montenotte SV |
| Via Monte Rosa 154 - 10154 Torino TO | Via Demetrio Cosola 12 - 10034 Chivasso TO |
| Via Isonzo 112 - 10141 Torino TO | Viale Marconi 68 - 08045 Lanusei OG |
| Via Ugo La Malfa 99 - 90147 Palermo PA | Via Dei Cinque Archi Snc – 00049 Velletri RM |
| Centro Direzionale - Isola F7 - 80143 Napoli NA | Via Olimpia 27 - 00015 Monterotondo RM |
| Cdn Citt. Delle Tel. Is. F6 - 80143 Napoli NA | Via Camassa Snc - 73100 Lecce LE |
| Via Della Boscaiola 26 - 20159 Milano MI | Via Luigi Gallo 18/A - 12100 Cuneo CN |
| Via Tonale 11 - 20125 Milano MI | Via S. Agata 146 - 87027 Paola CS |
| Via Antonio Pacinotti 57 - 90145 Palermo PA | Viale Antonio Gramsci 16 - 70056 Molfetta BA |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Via Carducci 22 – 30172 Venezia VE | Via Santa Maria In Via 6 - 00187 Roma RM |
| Via7^ Strada 22-Ed.Sirio - 35122 Padova PD | Via Del Popolo 71 - 19126 La Spezia SP |
| Via Di Ripoli 266 - 50126 Firenze FI | Via Sorrento 30 - 00055 Ladispoli RM |
| Via Calamattia 17 - 09134 Cagliari CA | Via Leon Battista Alberti 29 - 10022 Carmagnola TO |
| Via Tripoli 94 - 10137 Torino TO | Fosso dell'Osa SNC - 00132 Roma RM |
| Via Vincenzo Lancia 55 - 10141 Torino TO | Via Napoli Snc - 71016 San Severo FG |
| Via Ugo La Malfa 159 - 90147 Palermo PA | Via Paolo Toschi 27 - 42100 Reggio Emilia RE |
| Via Piero Maroncelli 1 - 40126 Bologna BO | Via Sardegna 2 - 63100 Ascoli Piceno AP |
| Via Giovanni Da Verrazzano Snc - 26900 Lodi LO | Via Giovanni XXIII 13 - 52027 San Giovanni Valdarno AR |
| Via Capo Di Lucca 46 - 40126 Bologna BO | Via Delle Biole snc - San Leo - 52100 Arezzo AR |
| Via Ricasoli 93 - 53100 Siena SI | Via Oriolo Romano 265 - 00189 Roma RM |
| Via Francesco Albani 3 - 40129 Bologna BO | Via Agostino Depretis 40 - 80133 Napoli NA |
| Via Cagliari 2 - 73014 Gallipoli LE | Via Spontini 59 - 00013 Mentana RM |
| Via Lamaro 79 - 00173 Roma RM | Via Torquato Tasso 121 - 24121 Bergamo BG |
| Via Irpinia 36 – 30174 Venezia VE | Via Viaccia 10 - 55100 Lucca LU |
| Via Torino 84 – 30172 Venezia VE | Via Tiso Da Camposampiero 23 - 35012 Camposampiero PD |
| Via della Stadera 66 - 80143 Napoli NA | Via Cosimo Morelli 19 - 62100 Macerata MC |
| Cdn Citt. Delle Tel. Is. F5 - 80143 Napoli NA | Via Rombon 52 - 20134 Milano MI |
| Via Pietro Oreste 20 - 70123 Bari BA | Via Santa Margherita 13 - 60131 Ancona AN |
| Via Della Bufalotta 241 - 00139 Roma RM | Via Leonardo Bianchi - 63039 San Benedetto del Tronto AP |
| Via San Giovanni Bosco 1 - 72100 Brindisi BR | Località Biscollai - 08100 Nuoro NU |
| Via7^ Strada 22-Ed.S.Barbara Torre B - 35122 Padova PD | Via Carlo Giuliozzi 34 - 62100 Macerata MC |
| Via Di Valleranello 1 - 00128 Roma RM | Via Casella 16 - 47838 Riccione RN |
| Via Antonio Meucci 17 - 48100 Ravenna RA | Via Tuderte snc - 06126 Perugia PG |
| Via Raffaele Mauri - 84131 Salerno SA | Via XX Settembre 161/R - 16100 Genova GE |
| Via dei Gelsomini Loc. Santo Cono - 88100 Catanzaro CZ | Via Ponte D'Oddi 9 - 06125 Perugia PG |
| Via Dei Ciclamini 38 - 20147 Milano MI | Via Pietro Mascagni 46 - 42100 Reggio Emilia RE |
| Via Virgilio 42 - 80053 Castellammare di Stabia NA | Via San Domenico snc - Santa Maria A - 62012 Civitanova Marche MC |
| Via Antonio Meucci 4/6 - 57124 Livorno LI | Via Boscone 320 - 47521 Cesena FC |
| Via Corfu' 81 - 25124 Brescia BS | Via Basilicata - 64026 Roseto degli Abruzzi TE |
| Via Vigonovese 107 - 35127 Padova PD | Via Don Petruio 46 - 60044 Fabriano AN |
| Via Vincenzo Lamaro 81 - 00173 Roma RM | Via Del Carabiniere 15 - 33170 Pordenone PN |
| Via San Francesco D'Assisi 35 - 00041 Albano Laziale RM | Via Giacomo Matteotti - 86170 Isernia IS |
| Via XXV Luglio 7 - 00046 Grottaferrata RM | Via Po 7 - 43100 Parma PR |
| Largo Valerio Bacigalupo 9 - 00142 Roma RM | Via Duca Del Mare 35 - 04100 Latina LT |
| Via Challant 38 - 10142 Torino TO | Via Digione 12 - 44029 Comacchio FE |
| Via Calamattia 19 - 09134 Cagliari CA | Via Brunenghi Snc - 17024 Finale Ligure SV |
| Via degli Estensi, 52 - 00164 Roma RM | Via Cabassi 2 - 41100 Modena MO |
| Via Tiburtina Valeria 419 - 65129 Pescara PE | Via Gran Sasso snc - 63018 Porto Sant'Elpidio FM |
| Via Marco Aurelio 24 - 20127 Milano MI | Via Baldasseria Bassa 46 - 33100 Udine UD |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Viale Croce Snc - 84015 Nocera Superiore SA | Via IV Novembre - 86100 Campobasso CB |
| Contrada Patacca - 80056 Ercolano NA | Via F. Niccolaioni 78 - 56025 Pontedera PI |
| Via Giuseppe Giacosa 19 - 20127 Milano MI | Via Dei Platani 23 – 55049 Viareggio LU |
| Viale Fra' Andrea Di Giovanni 14 - 00126 Roma RM | Via Mulinetto 9 - 44100 Ferrara FE |
| Via Tommaso Emaldi 21 - 48022 Lugo RA | Via Del Pallone 3 - 40126 Bologna BO |
| Via Leonardo Da Vinci 30 - 20060 Cassina De' Pecchi MI | Via Degli Albari 9 - 40126 Bologna BO |
| Via Fosso Pioppo 10 - 84091 Battipaglia SA | Via Piero Calamandrei snc - 61029 Urbino PU |
| Via Sacco e Vanzetti 129 - 00155 Roma RM | Via Gammarana - 64100 Teramo TE |
| Via Alessandro Manzoni 2 - 90133 Palermo PA | Via Radici In Piano 118 - 41049 Sassuolo MO |
| Viuzzo dei Bruni 6 - 50133 Firenze FI | Via Pablo Picasso Snc - 41037 Mirandola MO |
| Via Aldo Manuzio 13 -16143 Genova GE | Via della Repubblica snc - 06083 Bastia Umbra PG |
| Via Capodistria 6 - 20151 Milano MI | Via Leonardo Da Vinci Snc - 61043 Cagli PU |
| Via San Lorenzo 8 - 60027 Osimo AN | Via Madonna Delle Grazie - 86039 Termoli CB |
| Via Dante Alighieri 80 - 22100 Como CO | Via Angelo Siffredi 67 - 16153 Genova GE |
| Viale Alessandro Guidoni 42 - 50127 Firenze FI | Via Gian Giunio Parise - 31046 Oderzo TV |
| Via7^Strada 22-Ed.Raccordo Curvo - 35122 Padova PD | Via Milano 57 - Fraz. Paterno - 67051 Avezzano AQ |
| Via Saverio Landolina 50 - 90142 Palermo PA | Via Sticchi 13 - 62029 Tolentino MC |
| Via Guglielmo Reiss Romoli 274 - 10148 Torino TO | Via Palestro Snc -35138 Padova PD |
| Via Monte Viglio - 65124 Pescara PE | Via Delle Scalette Snc - 62032 Camerino MC |
| Via Carlo Gallini 30 – 27058 Voghera PV | Via Guglielmo Oberdan 20 - 64011 Alba Adriatica TE |
| Via Guido Miglioli 8 - 60131 Ancona AN | Via Puccini 13 - 38068 Rovereto TN |
| Via Ezio Maccani 86 - 38100 Trento TN | Via Delle Susine Snc - 00172 Roma RM |
| Via Della Biscia 226 - 35136 Padova PD | Via Madonna Dell'Asilo - 66054 Vasto CH |
| Via Egidio Folli 17 - 20134 Milano MI | Via Enrico Fermi 2 - 06128 Perugia PG |
| Misterbianco - 95100 Misterbianco CT | Via Provinciale snc -54033 Carrara MS |
| Via Tonale 27 - 23900 Lecco LC | Via Liquirizia 1 - 66050 San Salvo CH |
| Via Wenner 24 Zona Industriale - 84131 Salerno SA | Via Caravaggio Snc - 42100 Reggio Emilia RE |
| Via Giotto 22 - 40133 Bologna BO | Via Salvatore Dau 2 - 07100 Sassari SS |
| Via Timavo 39 - 80126 Napoli NA | Via Caduti Per La Libertà - 248015 Cervia RA |
| Via Grazia Deledda 32 - 30027 San Donà di Piave VE | Via Valentina Zambra 1 - 38100 Trento TN |
| Via Plauto 29 - 90148 Palermo PA | Via Opifici snc - 55045 Pietrasanta LU |
| Via Esiodo 2 – 30173 Venezia VE | Via Luigi Luciani 29 - 63039 San Benedetto del Tronto AP |
| Via Francesco Vigo Pellizzari 30 – 20871 Vimercate MB | Via degli Appennini 9 - 93012 Gela CL |
| Via Suor Luigia Grassi 13 - 27100 Pavia PV | Via Nazario Sauro Snc - 85100 Potenza PZ |
| Via Sant'Orsola 5 - 24122 Bergamo BG | Via Paternostro snc - 88900 Crotone KR |
| Piazzale Donatori Sangue 6 – 30171 Venezia VE | Traversa Lacquari Snc – 89900 Vibo Valentia VV |
| Corso IV Novembre 64 - 10098 Rivoli TO | Via Foschini 3 - 80077 Ischia NA |
| Contrada Bue Marino Snc - 91017 Pantelleria TP | Via Tre Monti 29 - 98057 Milazzo ME |
| Via Assisi 160 - 00181 Roma RM | Via Taranto 96 - 73100 Lecce LE |
| Via Caduti Del Lavoro B 40 - 60131 Ancona AN | Via Perugia 101 - 83035 Grottaminarda AV |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of
IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address)***

| | |
|---|---|
| Via Romania 46 - 47900 Rimini RN | Viale Candelaro 34 - 71100 Foggia FG |
| Via Henri Beyle Stendhal 31 - 40128 Bologna BO | Via Hermada Snc - 71043 Manfredonia FG |
| Via Strinella 2 - 67100 L'Aquila AQ | Via Marchese di Montrone 123 - 70121 Bari BA |
| Viale Giovine Italia 9/r - 50122 Firenze FI | Via Colapesce 36 - 98121 Messina ME |
| Via Fratelli Rey 1 - 17100 Savona SV | Via Giovanni Verga 4 - 74123 Taranto TA |
| Via Bonanni 28 - 01033 Civita Castell. VT | Via Licinella Snc - 84047 Capaccio SA |
| Via Sante Zanon 7 - 31100 Treviso TV | Viale Italia 274 - 96011 Augusta SR |
| Viale Toscana 3/5 - 20089 Rozzano MI | Via Schiavello (Contrada Giardini) - 87012 Castrovillari CS |
| Via Le Murie Snc - 26013 Crema CR | Via San Francesco D'Assisi Snc - 74019 Palagiano TA |
| Via Resia 188 - 39100 Bolzano BZ | Via Martiri Della Libertà 1 - 43013 Langhirano PR |
| Via Marco Aurelio 28 - 20127 Milano MI | Via Croce Rossa snc - 98124 Messina ME |
| Via Bartolomeo Bianco 1 - 16127 Genova GE | Via Puglia, 75 - 75025 Policoro MT |
| Via Argine C/O Pal. D. Sport - 80146 Napoli NA | Via Minella 10 - 48012 Bagnacavallo RA |
| Via Luigi Mercantini 9 - 10121 Torino TO | Via Giuseppe Persiani Snc - 62017 Porto Recanati MC |
| Via Giovanni Vincenzo Gravina Snc - 00196 Roma RM | Via Galileo Galilei Snc - 85025 Melfi PZ |
| Via Leone XIII 30 - 93100 Caltanissetta CL | Via Masaccio 26 - 74100 Taranto TA |
| Viale Mediterraneo 56 - 30015 Chioggia VE | Via Cesare Micheli snc - 06049 Spoleto PG |
| Corso Giuseppe Garibaldi 120 - 20025 Legnano MI | Via Padre Semeria 220 - 18038 San Remo IM |
| Via Panebianco 297 - 87100 Cosenza CS | Via Moliterno Snc - 85042 Lagonegro PZ |
| Via Mentana 41 - 05100 Terni TR | Via Della Cesarina 282 - 00139 Roma RM |
| Via Ludovico Loquercio 38 - 70012 Bari BA | Via Provinciale Marina Grande 122 - 80073 Capri NA |
| Via Massimo Misani 8 - 33100 Udine UD | Viale Nuovo 19 - 40037 Sasso Marconi BO |
| Via Benedetto Biagi 8 - 71100 Foggia FG | Via Cesare Dattilo 3/5 - 16151 Genova GE |
| Via Cairoli 19 - 44100 Ferrara FE | Via Gianbattista Vico 36 - 09045 Quartu Sant'Elena CA |
| Via Pietro Donà 4 - 35129 Padova PD | Largo Volontari Del Sangue Snc - 61100 Pesaro PU |
| Via Francesco Guardione 111 - 90139 Palermo PA | Via Francesco Petrarca - 07021 Arzachena OT |
| Via Redipuglia snc -61100 Pesaro e Urbino PU | Via Bracco 8 - 44100 Ferrara FE |
| Via Diomede Carafa Snc - 80124 Napoli NA | Via Pozzuoli 1 - 41012 Carpi MO |
| Via Di Macchia Palocco 243 - 00125 Roma RM | Via Enrico Toti 6 - 40033 Casalecchio di Reno BO |
| Via Vittorio Emanuele 175 - 98035 Giardini Naxos ME | Strada Giordano Cavestro 8 - 43100 Parma PR |
| Via Michele Fusco 34 - 41100 Modena MO | Contrada Riposo snc - 89044 Locri RC |
| Via Andrea Mantegna 11 - 20154 Milano MI | Via Dei Monti - 53042 Chianciano Terme SI |
| Via Padulli 15 - 47100 Forlì FC | Corso Nazioni Unite 7 – 28922 Verbania VB |
| Via Di Tor Pagnotta 68 - 00143 Roma RM | Via Aguzzafame 75 – 27029 Vigevano PV |
| Via Ramaglia, snc - 80145 Napoli NA | Via della Concordia 5 - 21052 Busto Arsizio VA |
| Via Passariello Snc - 80038 Pomigliano D'Arco NA | Via Tripoli 18 - 15100 Alessandria AL |
| Via Picena - 66100 Chieti CH | Viale Giulio Cesare 349 - 28100 Novara NO |
| Piazzale Mater Ecclesiae 5 - 70124 Bari BA | Via Postumia 2/E - 26100 Cremona CR |
| Via Del Pallone 5 - 40126 Bologna BO | Via Tonale angolo via Morbegno 3 - 23100 Sondrio SO |
| Via Della Basilica Romana 1 - 00036 Palestrina RM | Via Barca San Domenico Snc - 03039 Sora FR |

Data revisione
*Revision date* 14.10.2019

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address)***

| | |
|---|---|
| Via Galatina Snc - San Clemente - 81100 Caserta CE | Via Martiri della Libertà 15 - 28041 Arona NO |
| Via Fiume Bianco 8 - 00144 Roma RM | Viale Lombardia 9 - 23807 Merate LC |
| Via Comacchio 133 - 44100 Ferrara FE | Via Trincea Dei Razzi 77 - 09122 Cagliari CA |
| Via Duca D'Aosta 7 - 82100 Benevento BN | Via Pescheria 17 - 46100 Mantova MN |
| Via Orazio Benedetto De Saussure 1 - 24126 Bergamo BG | Via Calamandrei 15 - 51018 Pieve a Nievole PT |
| Via Borgaro 21/27 -10149 Torino TO | Via Giuseppe Cesare Abba 1 - 25016 Ghedi BS |
| Via Tenente Alberti 64 - 91100 Trapani TP | Via Niccolò Machiavelli 16 - 15100 Alessandria AL |
| Via Monsignor Giovanni Fiorentini 5 - 88100 Catanzaro CZ | Via Fratelli Cairoli 62 - 23900 Lecco LC |
| Via Cisalpina Snc - 42100 Reggio Emilia RE | Via Carlo Viola, 65 - 11026 Pont-Saint-Martin AO |
| Via Quieta snc Ang. V.Novara - 95128 Catania CT | Piazza Giacomo Matteotti 4 - 28100 Novara NO |
| Via Santa Maria Del Campo 40 - 16035 Rapallo GE | Via Magolfa 8 - 20143 Milano MI |
| Via Vagnola 57 - 80058 Torre Annunziata NA | Via XXVI Febbraio 34 - 11100 Aosta AO |
| Via Bardet 47 - 65126 Pescara PE | Via Dei Martiri 5 - 20017 Rho MI |
| Via Carlo Forlanini 39 - 34139 Trieste TS | Viale Della Pace 9 - 11100 Aosta AO |
| Via Giuseppe Macaggi 12 - 16121 Genova GE | Via Senatore Ezio Vanoni 7 - 23017 Morbegno SO |
| Via Guglielmo Marconi 274 - 00146 Roma RM | Via Circonvallazione Sud 10/A - 46100 Mantova MN |
| Via Benedetto Croce Snc - 80014 Giugliano In Campania NA | Via Locatelli Milesi snc – 24018 Villa d'Almè BG |
| Via Maso Finiguerra 18 - 00173 Roma RM | Via Gian Antonio Bazzi 9 – 13100 Vercelli VC |
| Via Fontana 1 - 20122 Milano MI | Via Giovanni XXIII 1 - 62019 Recanati MC |
| Viale Stelvio 15 - 20159 Milano MI | Via Codignole 31 - 25124 Brescia BS |
| Via Giacomo Zanella 17 - 35013 Cittadella PD | Via Moretto 46 - 25121 Brescia BS |
| Via Ginibissa 12 - 20081 Abbiategrasso MI | Via Cesare Battisti 6 - 21023 Besozzo VA |
| Via Francesco Crispi 7 - 34170 Gorizia GO | Via Giacosa 6 - 10086 Rivarolo Canavese TO |
| Viale Liegi 31/A - 00198 Roma RM | Piazza Cesare Battisti 38/41 - 15033 Casale Monferrato AL |
| Via Della Rosolina 76 A - 00012 Tivoli RM | Via Fratelli Rosselli 74 - 13900 Biella BI |
| Via Piave 36 - 94100 Enna EN | Via Cesare Bettini 4 - 25038 Rovato BS |
| Piazza Luigi Vanvitelli 7 - 80129 Napoli NA | Via Armando Battistini 39 - 47021 San Piero in Bagno FC |
| Via Giovanni Battista Quadri 121 – 36100 Vicenza VI | Via Antica Di Cassano 1 - 20060 Cassina De' Pecchi MI |
| Via Petrarca 32 - 52100 Arezzo AR | Via Giuseppe Ferrari 34 - 20900 Monza MB |
| Viale Luigi Borri 150 – 21100 Varese VA | Via Virgilio 7 - 25041 Darfo Boario Terme BS |
| Viale Italia 67 - 10040 Leini TO | Via Leone Leoni 53 - 22017 Menaggio CO |
| Via Erodoto 1 - 20096 Pioltello MI | Via Luigi Scala 1 - 12037 Saluzzo CN |
| Via Giustino Fortunato 5 - 75100 Matera MT | Viale Giovanni Amendola 2 - 28845 Domodossola VB |
| Corso Stamira 46 - 60122 Ancona AN | Via Del Perilasio Snc - 06024 Gubbio PG |
| Viale Brutium Snc - 88100 Catanzaro CZ | Corso Leoniero 62/b -15067 Tortona AL |
| Via Giovanni Battista Bongioanni 17 - 12100 Cuneo CN | Via Francesco Ferrucci 1 - 10093 Collegno TO |
| Via Caudina Snc - 81024 Maddaloni CE | Via Giuseppe Verdi 8 - 12084 Mondovì CN |
| Via Salvatore Cognetti De Martiis 51 - 10149 Torino TO | Via Pergolesi 10 fraz. Vighizzolo - 22063 Cantù CO |
| Via Due Principati 5 - 83100 Avellino AV | Via Giovanni XXIII 8 - 20077 Melegnano MI |
| Via Conte Rosso 20 - 86100 Campobasso CB | Viale Ettore Andreis 45 - 25015 Desenzano del Garda BS |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Viale Piombino snc - 50142 Firenze FI | Via Aldo Moro 14 - 25043 Breno BS |
| Corso Domenico Baccarini 13 - 48018 Faenza RA | Piazza Dante Alighieri 10 Bis - 10023 Chieri TO |
| Via Raffaele Mauri 201 - 84132 Salerno SA | Via Rovigo 10 - 20132 Milano MI |
| Via Portuense 709 - 00148 Roma RM | Via Antonio Gramsci 56 - 20032 Cormano MI |
| Via Bartolomeo Marliano 27 - 00162 Roma RM | Via Giorgio Gusmini 35 - 24023 Clusone BG |
| Via Etnea 47 - 95131 Catania CT | Via Don Scaglione 21 - 12051 Alba CN |
| Via Trieste 6 -10043 Orbassano TO | Via Tevere 16 - 20900 Monza MB |
| Via Checco Durante 4 - 00177 Roma RM | Via Delle Forze Armate 390 - 20152 Milano MI |
| Viale Europa snc - 97100 Ragusa RG | Via Aurora 8 - 20037 Paderno Dugnano MI |
| Via Carlo Goldoni 6 - 45100 Rovigo RO | Piazza Virginio Rufo 6 - 22036 Erba CO |
| Via Della Montagnola 29 - 60131 Ancona AN | Via Della Resistenza 88 – 41058 Vignola MO |
| Viale Ludovico Canali 10 - 02100 Rieti RI | Via Monte Navale 1 -10015 Ivrea TO |
| Piazza Cordusio snc - 20123 Milano MI | Via Francesco Flarer 35 - 27100 Pavia PV |
| Via Stadio 14 - 37047 San Bonifacio VR | Via Guglielmo Marconi 10 - 12042 Bra CN |
| Via Pra 8 - 16157 Genova GE | Via Giacomo Matteotti 1 - 23022 Chiavenna SO |
| Via Consolare Latina 54 - 00034 Colleferro RM | Via Papa Giovanni XXIII 5 - 45011 Adria RO |
| Via Aldo Moro Snc - 80018 Mugnano Di NA NA | Via Cesare Balbo 8 - 20136 Milano MI |
| Viale Monte Ceneri 68 - 20155 Milano MI | Via Privata Stazione 5/5 - 13011 Borgosesia VC |
| Via Armando Diaz 55 - 90011 Bagheria PA | Via Principe Amedeo 62 - 10026 Santena TO |
| Via Milano - 65122 Pescara PE | Via Loreto 23/25 - 28021 Borgomanero NO |
| Via Giovanni Verga 1 - 81031 Aversa CE | Via Tenente Francesco Melpignani Snc - 72017 Ostuni BR |
| Via Don Luigi Guanella 9 - 20128 Milano MI | Via Papa Giovanni XXIII Snc - 76121 Barletta BT |
| Via Arturo Toscanini 32 - 30016 Jesolo VE | Via Paolo Bignami 2/A - 26845 Codogno LO |
| Contrada Must - 98066 Patti ME | Via Canonico Del Drago 89 - 70043 Monopoli BA |
| Via Belfiore 13 - 20145 Milano MI | Via Francesco Rossi Snc - 76012 Canosa Di Puglia BT |
| Via Antonio Meucci Snc - 89015 Palmi RC | Via Bari 5 - 10144 Torino TO |
| Via Giuseppe Bignami,40 - 00054 Fiumicino RM | Corso Umberto 45 -13043 Cigliano VC |
| Via Canavesio 4 - 10064 Pinerolo TO | Via Marzanica 98 - 24124 Bergamo BG |
| Via Edoardo Bonardi 16 - 15100 Alessandria AL | Via Luigi Mercantini 5 - 10121 Torino TO |
| Via Del Patriota snc - 54100 Massa MS | Via Francesco Baracca snc - 70042 Mola di Bari BA |
| Via Gaspare Mignosi snc - 90134 Palermo PA | Via Pirro - 74100 Taranto TA |
| Corso Cavour 1 - 98122 Messina ME | Via Boemondo Normanno Snc - 72019 San Vito dei Normanni BR |
| Via Nino Bixio 30 - 16043 Chiavari GE | Via Malennio Snc - 73100 Lecce LE |
| Via Dei Testa 7/9 - 10051 Avigliana TO | Via Dante Alighieri 214 - 70019 Triggiano BA |
| Via Emilia Levante 79 - 40139 Bologna BO | Via Privata Alle Ville 5 - 28831 Baveno VB |
| Cdn Citt. Delle Tel. Is. B1 - 80143 Napoli NA | Via Giacomo Matteotti 41 - 13836 Cossato BI |
| Via Caduti Sul Lavoro 45 - 29100 Piacenza PC | Via XX Settembre 2 - 12051 Alba CN |
| Via Villagrazia 405 - 90126 Palermo PA | Corso Africa snc – 24040 Verdellino BG |
| Salita Scudillo 18 - 80131 Napoli NA | Via Nazionale 138 - 23823 Colico LC |
| Via Ala 14 - 95123 Catania CT | Via Bizzarri Snc - 74024 Manduria TA |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Via Valle Fioretta 205 - 03100 Frosinone FR | Via Giovanni XXIII 13 - 50032 Borgo San Lorenzo FI |
| Via Catusi, snc (angolo via Mazzini) - 92019 Sciacca AG | Via F.Chopin - San Pietro in Cariano - 37029 San Pietro in Cariano VR |
| Via Martiri Della Libertà 5 - 25068 Sarezzo BS | Via Daniele Manin 33 - 51016 Montecatini Terme PT |
| Via Carlo Del Prete 141 - 50127 Firenze FI | Via Claudio Monteverdi 12 - 50144 Firenze FI |
| Via Tenutella Snc - 00041 Albano Laziale RM | Via Pianezza 59 - 10091 Alpignano TO |
| Via Enrico Dandolo 12 - 31100 Treviso TV | Via Tripoli 96 - 10137 Torino TO |
| Via Torino 5 - 21047 Saronno VA | Via Giovanni Sforza 10 - 54027 Pontremoli MS |
| Via Giovanni Pascoli 9 - 34138 Trieste TS | Via Ernestro Nathan 110 - 00146 Roma RM |
| Via Polveriera 157 - 80035 Nola NA | Via Cesare Cantu, snc - 91026 Mazara del Vallo TP |
| Via Marino Torre 32 - 91100 Trapani TP | Via A.Moro 16 - 95030 Sant'Agata Li Battiati CT |
| Strada Caldarola 18 - 70126 Bari BA | Via Ardita 11 - 95024 Acireale CT |
| Via Rolih 2/A - 16163 Genova GE | Via Francesco Crispi 40 - 98050 Santa Marina Salina ME |
| Via Lupiae 50 - 73100 Lecce LE | Via Filippo Mancuso Snc - 98055 Lipari ME |
| Via Libertà 37 - 90146 Palermo PA | Via Fra' Cherubino da Caltagirone 6 - 95041 Caltagirone CT |
| Via Monte Di Dio 38 - 80132 Napoli NA | Contrada Santa Barbara - 90015 Cefalù PA |
| Via Torre Di Mizzo Loc Mungivacca - 70126 Bari BA | Via Pietro Lombardo 43 - 91011 Alcamo TP |
| Via Pineta Sacchetti 229 - 00168 Roma RM | Via G. Nicastro 20 - 97100 Ragusa RG |
| Via Mascagni Ang. Madonna Della Croce - 70022 Altamura BA | Via Curtatone e Montanara 10 - 50053 Empoli FI |
| Via7^Strada 22-Ed.S.Barbara Torre A - 35122 Padova PD | Via Resistenza Partigiana, snc - 97015 Modica RG |
| Via Alessandro Manzoni 6 - 22063 Cantù CO | Via Dei Carlini 2A - 33100 Udine UD |
| Via Del Cinematografo Loc. Falasche - 00042 Anzio RM | Contrada Capo Grecale - 92010 Lampedusa e Linosa AG |
| Aeroporto Fiumicino - 00054 Fiumicino RM | Via Giuseppe Mazzini 35 - 92010 Lampedusa e Linosa AG |
| Via Tunisi, snc - 91025 Marsala TP | Via Maratona - 00053 Civitavecchia RM |
| Via Feronia 104 - 00157 Roma RM | Via Madonnetta Snc - 36075 Montecchio Maggiore VI |
| Viale Murge Snc - 76123 Andria BT | Corso Matteotti 1 - 21018 Sesto Calende VA |
| Via Matteo Maria Boiardo 12 - 09128 Cagliari CA | Via del Crocifisso 30 - 21049 Tradate VA |
| Via Mons. Domenico Orlando 10 - 95126 Catania CT | Via Guglielmo Marconi 10 - 26041 Casalmaggiore CR |
| Via Casetta Mattei 53 - 00148 Roma RM | Via Gian Battista Scalabrini 22 - 22100 Como CO |
| Via Arnaldo da Brescia (ang. V.Savona) - 21052 Busto Arsizio VA | Via Luigi Einaudi 4 - 31015 Conegliano TV |
| Via Felice Cavallotti 2 - 21013 Gallarate VA | Via Dante Alighieri Snc - 52011 Bibbiena AR |
| Via Igino Garbini Snc - 01100 Viterbo VT | Via Franchino Gaffurio 3 - 27100 Pavia PV |
| Via Molise 17 - 20900 Monza MB | Viale Dei Caduti 101 - 37045 Legnago VR |
| Via Del Brennero – Figuretta - 56123 Pisa PI | Via Giovanbattista Cima - 34074 Monfalcone GO |
| Contrada San Giusippuzzu snc - 92100 Agrigento AG | Via Giovanni De Giorgio - 07041 Alghero SS |
| Via Sofonisba Anguissola 11 - 26100 Cremona CR | Via Baccanelle 6 - 55032 Castelnuovo di Garfagnana LU |
| Via Guglielmo Oberdan 20 - 40126 Bologna BO | Via Martiri Libertà 45 - 18100 Imperia IM |
| Via San Francesco Snc - 73031 Alessano LE | Via Alessandro La Marmora - 00053 Civitavecchia RM |
| Salita Di Gretta 36 -34136 Trieste TS | Località Val Calda snc - 32044 Pieve di Cadore BL |
| Sestriere Di Santa Croce 1302 - 30135 Venezia VE | Via Santa Teresa D'Avila 5 - 35028 Piove di Sacco PD |
| Via Calzaiuoli 114-118 - 50122 Firenze FI | Via Orcagna - 58100 Grosseto GR |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Piazza del Mercato 3 - 30031 Dolo VE | Calle Delle Ballotte 4870 – 30124 Venezia VE |
| Via A. Rubino – 84078 Vallo della Lucania SA | Via delle Fabbriche 8 - 39031 Brunico BZ |
| Via San Domenico 9 - 81037 Sessa Aurunca CE | S.S.148 Pontina Km 29,100 - 00040 Pomezia RM |
| Via Mascalucia 16 - 96100 Siracusa SR | Via Don Enrico Tazzoli - 09170 Oristano OR |
| Cdn Citt. Delle Tel. Is. F2 - 80143 Napoli NA | Via del Molinuzzo 13 - 51100 Pistoia PT |
| Via Stefano Da Seregno 39 - 20831 Seregno MB | Via Dante 20 - 39042 Bressanone BZ |
| Via Valle Del Silenzio Snc - 03014 Fiuggi FR | Via Pietro Mascagni Snc - 04011 Aprilia LT |
| Via Monteripido snc - 06125 Perugia PG | Via Crocifisso Snc - 09010 Iglesias CI |
| Via Novi 6 - 10152 Torino TO | Via Gaetano Negri 8 - 20123 Milano MI |
| Corso Europa 16 - 16132 Genova GE | Via Lombardia 7 - 07029 Tempio Pausania OT |
| Via Manetti 4 - 58100 Grosseto GR | Sestriere Di Santa Croce 1303/B – 30135 Venezia VE |
| Via Carducci 24 – 30172 Venezia VE | Via Riccardo Fabbri 1 - 00053 Civitavecchia RM |
| Via Sarcinello Ravagnese - 89015 Reggio Calabria RC | Via Santa Maria Segreta 3 - 20123 Milano MI |
| Via Flaminia 3 - 61032 Fano PU | Via Italo Montemezzi 18 - 37012 Bussolengo VR |
| Via Salvo d'Acquisto snc - 63023 Fermo FM | Borgo Santo Stefano 17 – 56048 Volterra PI |
| Corso Casale 203 -14100 Asti AT | Via G. Matteotti 1 Loc. Motecerboli - 56045 Pomarance PI |
| Via Montello 11 – 17019 Varazze SV | Via Giuseppe Belluzzo 12A – 37132 Verona VR |
| Via Galanta 13 - 20066 Melzo MI | Via Braccianese Claudia Km.22 - 00062 Bracciano RM |
| Via Bersaglio 19 - 39012 Merano BZ | Via Giovanni Battista Quadri 119/G – 36100 Vicenza VI |
| Via Giuseppe Palombini 54 - 00165 Roma RM | Via Belfiore 4 - 36015 Schio VI |
| Via Medaglie D'Oro 76 - 47100 Forlì FC | Via Mosca 8 - 07100 Sassari SS |
| Via Reggio Campi 93/A - 89126 Reggio Calabria RC | Via Gino Capponi 20 - 57121 Livorno LI |
| Via Sant'Agata 2 -18100 Imperia IM | Via Francesco Zappetti - 30026 Portogruaro VE |
| Via Dei Carlini 4 -33100 Udine UD | Via Giovanni Paolo II - 53035 Monteriggioni SI |
| Viale Della Pineta - 65129 Pescara PE | Via Val Chiarsò Snc - 33028 Tolmezzo UD |
| Via Ignazio Marabitti 1 - 96100 Siracusa SR | Via Rio snc - 32032 Feltre BL |
| Via George Sand 28 - 20161 Milano MI | Via Genova 31 -00184 Roma RM |
| Via Trento 86/A - 25128 Brescia BS | Via Val di Lanzo snc - 00141 Roma RM |
| Via Matteotti Snc - 02047 Poggio Mirteto RI | Località Bonu Trau - 08015 Macomer NU |
| Via Giuseppe Mazzini 5 - 24047 Treviglio BG | Via Alcide de Gasperi 70 - 38023 Cles TN |
| Staz. Centrale Piazza duca D'Aosta - 20124 Milano MI | Via Degli Artigiani 4 - 53036 Poggibonsi SI |
| Via Del Verde - 66034 Lanciano CH | Via Lucania Snc - 09013 Carbonia CI |
| Via Enrico Dandolo 14 - 31100 Treviso TV | Viale Europa - 04019 Terracina LT |
| Via del Cottolengo, 61 - 00165 Roma RM | Via Enea - 04016 Sabaudia LT |
| Viale Del Galoppatoio Snc - 00197 Roma RM | Via Grazia Deledda 13 - 09025 Sanluri VS |
| Via Cesare Battisti 56 - 64011 Alba Adriatica TE | Via Sarnano 29 - 00156 Roma RM |
| Via Buzzanca 32 - 90145 Palermo PA | Via Ugo La Malfa - 07014 Ozieri SS |
| Via Monti Lepini 29 - 04100 Latina LT | Via Fra' Paolo Sarpi - 33078 San Vito al Tagliamento PN |
| Via Felice Giani 2 - 60035 Jesi AN | Via Guglielmo Marconi 5 - 00040 Pomezia RM |
| Via Napoli 331 - 70123 Bari BA | Via Nino Bixio 1 - 53100 Siena SI |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Via Dei Castelli Romani 7 - 00042 Pomezia RM | Via Alessandro Manzoni 45 - 33053 Latisana UD |
| Loc. Bellafemmina snc - 88046 Lamezia Terme CZ | Via Della Rinascita Snc - 09030 Elmas CA |
| Via Calata Capodichino 52 - 80141 Napoli NA | Via Loreto 27 - 32100 Belluno BL |
| Via Ettore Majorana snc - 50053 Empoli FI | Via Fiume Snc - 09045 Quartu Sant'Elena CA |
| Via Leopardi snc - 58022 Follonica GR | Via Cina 5 - 00144 Roma RM |
| Via Claudio Fermi 52 - 07100 Sassari SS | Via Marmolaia 20 - 38033 Cavalese TN |
| Via Amico Aspertini 352 - 00133 Roma RM | Via Giacomo Matteotti Snc - 53048 Sinalunga SI |
| Via Giuseppe Belluzzo 12B - 37132 Verona VR | Via Italia, 16 - Loc. Camucia - 52042 Cortona AR |
| Via Albaro 97 - 16145 Genova GE | Via Generale Leoncini 1 - 57037 Portoferraio LI |
| Corso Alcide De Gasperi 421 - 70125 Bari BA | Via Giacomo Matteotti 36 - 32100 Belluno BL |
| Via Giorgio Vasari 19 - 20135 Milano MI | Via Angeli Custodi - 18019 Vallecrosia IM |
| Via Walter Procaccini 67 - 00173 Roma RM | Via Giacomo Matteotti 30 - 32100 Belluno BL |
| Via Cascina Bellaria 4 - 20151 Milano MI | Viale Venezia 27 -33033 Codroipo UD |
| Via Piave snc - 24020 Rovetta BG | Via Oristano snc - 08048 Tortolì OG |
| Via Del Coppetta 5 - 06124 Perugia PG | Viale Europa 8 - 16015 Casella GE |
| Via della Pace SNC - 70023 Gioia del Colle BA | Via Divisione Nino Nannetti 29 – 31029 Vittorio Veneto TV |
| Via Tomasi Di Lampedusa 191 - 51100 Pistoia PT | Via Enrico Dandolo 12/b - 31100 Treviso TV |
| Via Circonv.ne Orientale 58/A - 67039 Sulmona AQ | Loc. Barcara Circ. Dante Alighieri - 54011 Aulla MS |
| Corso Casale 223 - 14100 Asti AT | Via Fedele Soldani 23 - 50137 Firenze FI |
| Via Ernesto Ragazzoni 4 - 28100 Novara NO | Via De Tortisani 10 -Lido Di Venezia – 30126 Venezia VE |
| Via Carlo Baffi 1 - 71100 Foggia FG | Via Bergamo 17 - 39100 Bolzano BZ |
| Via Gaetano Mazzoni 62 - 00166 Roma RM | Via Loredan Snc - 33057 Palmanova UD |
| Via Roma 18 - 10121 Torino TO | Via Principe Amedeo 8 - 00044 Frascati RM |
| Galleria Vittorio Emanuele Snc - 20121 Milano MI | SS Dell'Amiata 323 - 58031 Arcidosso GR |
| Via Antonio Gramsci 7 - 38100 Trento TN | Via Oriolo Romano 250 - 00189 Roma RM |
| Via G. Nicastro 16 - 97100 Ragusa RG | Via Vittorio Veneto snc - 52100 Arezzo AR |
| Via Edmondo De Amicis 67 - 10093 Collegno TO | Via Angelo Emo 13/A - 00136 Roma RM |
| Corso Inghilterra, 66 - 10059 Susa TO | Via Lacriscia Snc - 03032 Arce FR |
| Via Roma 25/27 - 10073 Ciriè TO | Via Dei Lanifici 5/E – 36078 Valdagno VI |
| Via Della Bufalotta 247 - 00139 Roma RM | Via Pedetliva 14 - 39046 Ortisei BZ |
| Via Forlanini 10 A - 57025 Piombino LI | Via Degli Anselmi 3 - 50123 Firenze FI |
| Via Severini Snc - 80078 Pozzuoli NA | Via Giovanni Battista Quadri 119/C - 36100 Vicenza VI |
| Via delle Fonti 177 - 59100 Prato PO | Via Scipione Ammirato 33 - 50136 Firenze FI |
| Via Belvedere 2 - 40026 Imola BO | Via Gianni Rodari Snc - 08038 Sorgono NU |
| Via Orbetello 30 - 10148 Torino TO | Via Daniele Manin 7 - 31044 Montebelluna TV |
| Via Campania 11 - 74121 Taranto TA | Via Abruzzo 12 - 31033 Castelfranco Veneto TV |
| Via Cassia 1810 - 00123 Roma RM | Via De Massari Snc - 37045 Legnago VR |
| Piazza Francesco Crispi 12 - 87100 Cosenza CS | Via Di Prosecco 2/2 - 34016 Trieste TS |
| Via Piave 30 - 36061 Bassano Del Grappa VI | Via Delle Vigne - 07046 Porto Torres SS |
| Via Duca Del Mare 33 - 04100 Latina LT | Via don Giovanni Bosco 5 - 36040 Sossano VI |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-105/19

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Unità operative/*Operational units***
**(Ragione sociale-Indirizzo Sito / *Registered name-Site address*)**

| | |
|---|---|
| Via Cappella snc - 85042 Lagonegro PZ | Via I Maggio 27 - 37010 Costermano VR |
| Via Delle Conce 10 - 00154 Roma RM | Piazza Della Concordia 5 - 63020 Falerone FM |
| Via Ducezio snc - 98124 Messina ME | Piazza Guglielmo Marconi 3 - 71042 Cerignola FG |
| Via Po 5/B - 43100 Parma PR | Via Tagaste Snc - 00121 Roma RM |
| Via Donato Bramante 2 - 47900 Rimini RN | Via Madonna Dei Cieli 32 - 88100 Catanzaro CZ |
| Piazzale Italia - S. Anna - 55100 Lucca LU | Via Battaglia Di Monte Lungo 1 - 70123 Bari BA |
| Via Giuseppe Mazzini 111 - 15067 Novi Ligure AL | Via Roma 21 - 70017 Putignano BA |
| Via Borea - 18038 San Remo IM | Via Dietro Monastero Snc – 71018 Vico Del Gargano FG |
| Via Erasmo Gattamelata, 45 - 00176 Roma RM | Via Francesco Redi 17 - 20129 Milano MI |
| Via Cardinal Sily 7 - 00165 Roma RM | Via delle Croci 30 - 01016 Tarquinia VT |
| P.zza dei Cinquecento st. Termini - 00185 Roma RM | Via Angelo Messedaglia 58/A – 37069 Villafranca di Verona VR |
| Via Sant'Antonio Snc - 24016 San Pellegrino BG | Via Oristano - 07020 Palau OT |
| Via Antonio Palladio - 07026 Olbia OT | La Villa In Badia Snc - 39033 Corvara In Badia BZ |
| Via Giannino Sessa 8 - 20142 Milano MI | Via Sommariva 20 - 32021 Agordo BL |
| Via Del Zotto 15 - 33052 Cervignano D.Fr UD | Via Gaetano Pellegrini 28 – 37136 Verona VR |
| Località Tufolosnc - 88900 Crotone KR | Via Guglielmo Marconi 15 - 33097 Spilimbergo PN |
| Via Ascatiello Snc - 04023 Formia LT | Corso Duca degli Abruzzi.24 - 10128 Torino TO |
| Via Torino 210/6 - 10042 Nichelino TO | Viale Andrea Doria, 6 - 95125 Catania CT |
| Contrada Savarino Via Turati - 93100 Caltanissetta CL | Via Dell'Imposto - 58014 Manciano GR |
| Via Della Maiolica 5 - 34125 Trieste TS | Via Vincenzo Gioberti 15 - 12051 Alba CN |
| Viale Europa Snc - 74015 Martina Franca TA | Via Senesi Snc - 50055 Lastra A Signa FI |
| Via S. Josemaria Escriva - 81055 Santa Maria Capua Vetere CE | Via Giuseppe Compagnoni 64 - 20129 Milano MI |
| Via Brenta 12 - 73024 Maglie LE | Via A. Martinelli 39 - 20811 Cesano Maderno MB |
| Viale Giovanni Suzzani 119 - 20162 Milano MI | Viale Francesco Bassani 10 - 36016 Thiene VI |
| Via Donatori Del Sangue 15 - 46040 Guidizzolo MN | Via Del Corso, 353 - 00186 Roma RM |
| Viale Mellini 1 - 25032 Chiari BS | Via Lanero 30 - 14049 Nizza Monferrato AT |
| Via Circonvallaz. 19 Reg. Brignire - 11027 Saint Vincent AO | Via Forlanini 10 B - 57025 Piombino LI |
| Piazza San Francesco D'Assisi - 610015 Ivrea TO | Via Ammiraglio Magnaghi snc - 07024 La Maddalena OT |
| Via Folcara Snc - 03043 Cassino FR | Vico San Mauro Snc - 08033 Isili CA |
| Via Filippo Corridoni 13 - 46100 Mantova MN | Via Sommarive, 18 (loc. Povo) - 38123 Trento TN |
| Via Wenner Snc - 84080 Pellezzano SA | Via Conte Appiano 14 - 71100 Foggia FG |

Data revisione
*Revision date* 14.10.2019

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

SI CERTIFICA CHE IL SISTEMA DI GESTIONE ANTICORRUZIONE DI

*IT IS HEREBY CERTIFIED THAT THE ANTI-BRIBERY MANAGEMENT SYSTEM OF*

## LEONARDO - SOCIETÀ PER AZIONI

PIAZZA MONTE GRAPPA 4 00195 ROMA (RM) ITALIA

NELLE SEGUENTI UNITÀ OPERATIVE / *IN THE FOLLOWING OPERATIONAL UNITS*

PIAZZA MONTE GRAPPA 4 00195 ROMA (RM) ITALIA

E UNITÀ OPERATIVE INDICATE NELLE PAGINE SUCCESSIVE/ *AND OPERATIONAL UNITS IN THE FOLLOWING PAGES*

È CONFORME ALLA NORMA / *IS IN COMPLIANCE WITH THE STANDARD*

## ISO 37001:2016

PER I SEGUENTI CAMPI DI ATTIVITÀ / *FOR THE FOLLOWING FIELD(S) OF ACTIVITIES*

RICERCA E SVILUPPO, PROGETTAZIONE, REALIZZAZIONE, PRODUZIONE, INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA ED ADDESTRAMENTO DI: SISTEMI INFORMATICI; APPLICAZIONI SW; SISTEMI INTEGRATI DI DIFESA TERRESTRE, NAVALE, AERONAUTICA E SPAZIALE; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI DI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHE' LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI. PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO. PROGETTAZIONE, PRODUZIONE, INSTALLAZIONE, RIPARAZIONE, ASSISTENZA E MANUTENZIONE DI SISTEMI E/O SOLUZIONI HARDWARE E SOFTWARE PER L'INTEGRAZIONE E GESTIONE DI RETI ICT SICURE CON APPLICAZIONI VERTICALI NEI SETTORI MILITARI, PROFESSIONALI, DELL'AVIONICA, DELLA CYBER SECURITY, DELLA SICUREZZA E DELL'AUTOMAZIONE. PROGETTAZIONE, SVILUPPO, COSTRUZIONE, ASSEMBLAGGIO, COLLAUDO E COMMERCIALIZZAZIONE DI PRODOTTI PER L'INDUSTRIA AEROSPAZIALE E DELLA DIFESA. REVISIONE, MANUTENZIONE E COLLAUDO DI PRODOTTI E SISTEMI PER L'INDUSTRIA AEROSPAZIALE E DELLA DIFESA SIA NEI SITI LEONARDO SIA PRESSO FORNITORI, PARTNER E UTILIZZATORI FINALI. EROGAZIONE SERVIZI DI SUPPORTO POST VENDITA, QUALI PROGETTAZIONE, FORMAZIONE, FORNITURA DI MANUALI.

*RESEARCH AND DEVELOPMENT, DESIGN, CONSTRUCTION, PRODUCTION, INSTALLATION, COMMISSIONING, MAINTENANCE, ASSISTANCE AND TRAINING OF: IT SYSTEMS; SOFTWARE APPLICATIONS; INTEGRATED LAND, NAVAL, AERONAUTICS AND SPACE DEFENSE SYSTEMS, CIVIL AND MILITARY CONTROL SYSTEMS, LOCALIZATION SYSTEMS FOR MILITARY AND CIVIL APPLICATION; RELEVANT SUBSYSTEMS AND DEVICES. DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATED FOUNDATIONS, REINFORCED CONCRETE MANUFACTURED GOODS, PREFABRICATED BUILDINGS AND RELATED TECHNOLOGICAL SYSTEMS NECESSARY FOR COMMISSIONING. DESIGN, PRODUCTION, INSTALLATION, REPAIR, ASSISTANCE AND MAINTENANCE OF HARDWARE AND SOFTWARE SOLUTIONS FOR THE INTEGRATION AND MANAGEMENT OF SECURE ICT NETWORKS WITH VERTICAL APPLICATIONS IN THE MILITARY, PROFESSIONAL, AVIONICS, CYBER SECURITY, SECURITY AND AUTOMATION SECTORS. DESIGN, DEVELOPMENT, CONSTRUCTION, ASSEMBLY, TESTING AND MARKETING OF PRODUCTS FOR THE AEROSPACE AND DEFENSE INDUSTRIES. REVIEW, MAINTENANCE AND TESTING OF PRODUCTS AND SYSTEMS FOR THE AEROSPACE AND DEFENSE INDUSTRIES BOTH AT LEONARDO AND AT SUPPLIERS, PARTNERS AND END USERS SITES. AFTER-SALES SUPPORT SERVICES SUCH AS DESIGN, TRAINING, MANUALS.*

La validità del presente certificato è subordinata a sorveglianza periodica annuale / semestrale ed al riesame completo del sistema di gestione con periodicità triennale
*The validity of this certificate is dependent on an annual/six monthly audit and on a complete review, every three years, of the management system*

L'uso e la validità del presente certificato sono soggetti al rispetto del documento RINA: Regolamento per la Certificazione di Sistemi di Gestione Anticorruzione
*The use and validity of this certificate are subject to compliance with the RINA document: Rules for the Certification of Antibribery Management Systems*

| | | | |
|---|---|---|---|
| Prima emissione *First Issue* | 13.07.2018 | Data decisione di rinnovo *Renewal decision date* | 09.07.2021 |
| Data scadenza *Expiry Date* | 12.07.2024 | Data revisione *Revision date* | 27.07.2021 |

Paolo Teramo
Certification Italy Region Director

**RINA Services S.p.A.**
Via Corsica 12 – 16128 Genova Italy

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

**Altre unità operative coperte dal sistema di gestione di:**
***Other operational units covered by the management system of:***

# LEONARDO - SOCIETÀ PER AZIONI

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 37001:2016

CAMPI DI ATTIVITÀ / *FIELDS OF ACTIVITIES*

RICERCA E SVILUPPO, PROGETTAZIONE, REALIZZAZIONE, PRODUZIONE, INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA ED ADDESTRAMENTO DI: SISTEMI INFORMATICI; APPLICAZIONI SW; SISTEMI INTEGRATI DI DIFESA TERRESTRE, NAVALE, AERONAUTICA E SPAZIALE; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI DI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHE' LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI. PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO. PROGETTAZIONE, PRODUZIONE, INSTALLAZIONE, RIPARAZIONE, ASSISTENZA E MANUTENZIONE DI SISTEMI E/O SOLUZIONI HARDWARE E SOFTWARE PER L'INTEGRAZIONE E GESTIONE DI RETI ICT SICURE CON APPLICAZIONI VERTICALI NEI SETTORI MILITARI, PROFESSIONALI, DELL'AVIONICA, DELLA CYBER SECURITY, DELLA SICUREZZA E DELL'AUTOMAZIONE. PROGETTAZIONE, SVILUPPO, COSTRUZIONE, ASSEMBLAGGIO, COLLAUDO E COMMERCIALIZZAZIONE DI PRODOTTI PER L'INDUSTRIA AEROSPAZIALE E DELLA DIFESA. REVISIONE, MANUTENZIONE E COLLAUDO DI PRODOTTI E SISTEMI PER L'INDUSTRIA AEROSPAZIALE E DELLA DIFESA SIA NEI SITI LEONARDO SIA PRESSO FORNITORI, PARTNER E UTILIZZATORI FINALI. EROGAZIONE SERVIZI DI SUPPORTO POST VENDITA, QUALI PROGETTAZIONE, FORMAZIONE, FORNITURA DI MANUALI.

*RESEARCH AND DEVELOPMENT, DESIGN, CONSTRUCTION, PRODUCTION, INSTALLATION, COMMISSIONING, MAINTENANCE, ASSISTANCE AND TRAINING OF: IT SYSTEMS; SOFTWARE APPLICATIONS; INTEGRATED LAND, NAVAL, AERONAUTICS AND SPACE DEFENSE SYSTEMS, CIVIL AND MILITARY CONTROL SYSTEMS, LOCALIZATION SYSTEMS FOR MILITARY AND CIVIL APPLICATION; RELEVANT SUBSYSTEMS AND DEVICES. DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATED FOUNDATIONS, REINFORCED CONCRETE MANUFACTURED GOODS, PREFABRICATED BUILDINGS AND RELATED TECHNOLOGICAL SYSTEMS NECESSARY FOR COMMISSIONING. DESIGN, PRODUCTION, INSTALLATION, REPAIR, ASSISTANCE AND MAINTENANCE OF HARDWARE AND SOFTWARE SOLUTIONS FOR THE INTEGRATION AND MANAGEMENT OF SECURE ICT NETWORKS WITH VERTICAL APPLICATIONS IN THE MILITARY, PROFESSIONAL, AVIONICS, CYBER SECURITY, SECURITY AND AUTOMATION SECTORS. DESIGN, DEVELOPMENT, CONSTRUCTION, ASSEMBLY, TESTING AND MARKETING OF PRODUCTS FOR THE AEROSPACE AND DEFENSE INDUSTRIES. REVIEW, MAINTENANCE AND TESTING OF PRODUCTS AND SYSTEMS FOR THE AEROSPACE AND DEFENSE INDUSTRIES BOTH AT LEONARDO AND AT SUPPLIERS, PARTNERS AND END USERS SITES. AFTER-SALES SUPPORT SERVICES SUCH AS DESIGN, TRAINING, MANUALS.*

| **NOME DELLA DIVISIONE / *NAME OF DIVISION***<br>**(Ragione sociale-Indirizzo Sito / *Registered name-Site address)*** |
|---|
| **DIVISIONE AEROSTRUTTURE** |
| **Pomigliano d'Arco (NA) -** V.le dell'Aeronautica s.n.c. |
| **Grottaglie (TA)** - S.P. Grottaglie Monteiasi s.n.c. |
| **Foggia** - Loc. Incoronata s.n.c. |
| **Nola (NA) -** Zona ASI Loc. Boscofangone - Via Boscofangone s.n.c. |

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

| DIVISIONE VELIVOLI |
|---|
| **Roma -** Piazza Monte Grappa, 4 |
| **Torino** - Corso Francia, 426 |
| **Pomigliano d'Arco (NA) -** V.le dell'Aeronautica s.n.c. |
| **Caselle Torinese (TO),** Caselle Sud - Strada Malanghero |
| **Venegono Superiore (VA) -** Via Ing. Paolo Foresio, 1 |
| **Galatina (LE) -** Aeroporto Militare F. Cesari |
| **Roma** - Via Pastrengo, 20 |
| **Tessera (VE)** - Via Triestina, 214 |
| **Grottaglie (TA) -** S.P. Grottaglie Monteiasi s.n.c. |
| **Roma** - Via Flaminia, 135 |
| **Cameri (NO) -** Via Ticino snc |
| **Foggia** - Loc. Incoronata s.n.c. |
| **Lonate Pozzolo (VA),** Via del Gregge 100 |
| **Grosseto -** Aeroporto Aeronautica Militare "C. Baccarini" |
| **Latina** - Via dell' Aeroporto, 1 |
| **Venegono Inferiore (VA) -** Via F.lli Kennedy, 44 |

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

| DIVISIONE ELETTRONICA |
|---|
| **Roma -** Via Tiburtina Km 12,400 |
| **Genova** - Via G. Puccini, 2 |
| **La Spezia -** Via Valdilocchi, 15 |
| **Roma -** Via Laurentina, 760 |
| **Pomezia (RM) -** Viale dell'Industria, 4 |
| **Nerviano (MI) -** Viale Europa snc |
| **Campi Bisenzio (FI) -** Via delle Officine Galileo, 1 |
| **Bacoli (NA) -** Via Giulio Cesare, 105 |
| **Giugliano in Campania (NA) -** Circmuv. Esterna di Napoli |
| **Cisterna di Latina ( LT) -** ss 148 Pontina Km 62.200 |
| **Ronchi Dei Legionari (GO) -** LOC. Soleschiano Via Mario Stoppani, 21 |
| **Abbadia San Salvatore (SI) -** Via Hamman, 102 |
| **Montevarchi (AR)** - Via della Lama, 13 |
| **Chieti** - Via E. Mattei, 21 |
| **Taranto -** Viale del Lavoro, 101 |
| **Palermo** - Via di Villagrazia, 79 |
| **L'Aquila** - Via G.D. Cassini, 4 |
| **Catania -** Via Alfredo Agosta snc, Zona Ind. Pantano d'Arci |
| **Pisa** - Via di Marmiceto, 6c |
| **Lamezia Terme (CZ) -** Via Loriedo, 6 |
| **S. Maurizio Canavese (TO) -** strada Privata Aeroporto di Caselle |
| **Carsoli (AQ) -** Loc. Recocce Strada Provinciale Turanense Km. 44.452 |
| **La Spezia -** Viale Amendola 1, (Arsenale Militare Marittimo) |

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of
IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

**Livorno –** Via di Levante, 48

**Pozzuoli (NA) -** Via Monterusciello n. 75

**Portovenere (SP) -** Via Santa Maria 12

**Aulla (MS) -** Quartiere Gobetti, 53

**Brescia -** Via Lunga, 2

**DIVISIONE ELICOTTERI**

**Samarate (VA)**, Via G. Agusta n. 520

**Sesto Calende (VA)**, Via Indipendenza 2

**Vergiate (VA),** Via Roma 51

**Tessera (VE)** - Via Triestina, 214

**Frosinone -** Via Agusta, 1

**Roma** - Via Flaminia, 135

**Brindisi -** Contrada per Santa Teresa Pinti

**Pisa,** Via Cannizzaro 7 - Loc. Ospedaletto

**Anagni (FR),** Loc. Paduini s.n.c.

**Benevento**, Contrada Ponte Valentino ss 90bis

**Bresso (MI)** - Via Gian Carlo Clerici, 342

**Milano,** Viale dell' Aviazione, 65

**Roma -** Urbe, Via Salaria 825

**Samarate (VA),** Viale Adriatico 50

**Villasor (SU) -** Strada Statale 196, km 4 s.n.c.

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

| DIVISIONE CYBER SECURITY |
|---|
| **Roma -** Via Tiburtina Km 12,400 |
| **Torino** - C.so Marche |
| **Pomigliano d'Arco (NA) -** V.le dell'Aeronautica s.n.c. |
| **Genova** - Via G. Puccini, 2 |
| **Roma -** Via Laurentina, 760 |
| **Nerviano (MI) -** Viale Europa snc |
| **Campi Bisenzio (FI) -** Via delle Officine Galileo, 2 |
| **Bacoli (NA) -** Via Giulio Cesare, 105 |
| **Giugliano in Campania (NA) -** Circmuv. Esterna di Napoli |
| **Cisterna di Latina ( LT) -** SS 148 Pontina Km 62.201 |
| **Abbadia San Salvatore (SI) -** Via Hamman, 102 |
| **Montevarchi (AR)** - Via della Lama, 13 |
| **Brescia** - Via Lunga, 2 |
| **Chieti** - Via E. Mattei, 21 |
| **Taranto -** Viale del Lavoro, 101 |
| **L'Aquila** - Via G.D. Cassini, 4 |
| **Catania -** Via Alfredo Agosta snc, Zona Ind. Pantano d'Arci |
| **Pisa** - Via di Marmiceto, 6c |
| **Roma** - Via Faustiniana, 15-21-29 |
| **Quartucciu (CA)** - Loc. Pill'e Matta |
| **Sassari -** Via Giovanni Palatucci, 1 |
| **Lamezia Terme (CZ) -** Via Loriedo, 6 |
| **S. Maurizio Canavese (TO) -** Strada Privata Aeroporto di Caselle |
| **Napoli -** Via Bleriot, 82 |
| **Rende (CS)** - Via Pedro Alvares Cabrai, 14 |

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

# CERTIFICATO N. ABMS-27/18

# *CERTIFICATE No.*

| SEDI SECONDARIE |
|---|
| **Abbadia San Salvatore (SI)** - Via Hamman, 98 |
| **Augusta (SR)** - Via Capitaneria, 1 C/O Arsenale Marina Militare |
| **Bacoli (NA)** - Via Omero, 34 |
| **Bacoli (NA)** - Via Petronio Arbitro, 33/A |
| **Gioia del Colle (BA)** - Via Federico II di Svevia snc |
| **Latina** - Strada Borgo Sabotino s.n.c. |
| **Montesilvano (PE)** - Via Verrotti, 2/35 |
| **Piancastagnaio (SI)** - Loc. Podere San Martino, 170 |
| **Pomezia (RM)** - Aeroporto Militare De Bernardi |
| **Roma** - Via Barberini, 86 |
| **Roma** - Via di Castel Madama s.n.c. |
| **Roma** - Via Prestinari, 3/5/7 |
| **Roma** - Via Tiburtina, 1238 |
| **San Pietro a Patierno (NA)** - Via Nuova Tempio, 20 |
| **Tortona (AL)** - Via Postunia, 32 |
| **Treviso (TV)** - Via di Cannizzano, 22 |
| **Venezia** - Viale Alvise Ca' da Mosto, 29 - Fraz. Tessera |
| **Venegono Inferiore (VA)** - Campo Volo s.n.c. |
| **Genova -** c.so Ferdinando Maria Perrone 118 |
| **Cameri –** Aeroporto MIL. PAL. DLA 1 RMV SNC – Cameri |

Data revisione
*Revision date* 27.07.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SGQ N° 002 A

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale

*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. OHS-2835

# *CERTIFICATE No.*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

Si certifica che il Sistema di Gestione della Sicurezza e della Salute sul luogo di lavoro di

*It is hereby certified that the Occupational Health and Safety Management System of*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

PIAZZA MONTE GRAPPA, 4 00195 Roma (RM) ITALIA

nelle seguenti unità operative */ in the following operational units*

PRESSO I SITI INDICATI IN ALLEGATO
E PRESSO CANTIERI OPERATIVI

E UNITÀ OPERATIVE INDICATE NELLE PAGINE SUCCESSIVE */ AND OPERATIONAL UNITS IN THE FOLLOWING PAGES*

è conforme alla norma */ is in compliance with the standard*

## ISO 45001:2018

per le seguenti attività */ for the following activities*

RICERCA E SVILUPPO, PROGETTAZIONE, REALIZZAZIONE, PRODUZIONE, INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, CONSULENZA TECNICA ED ADDESTRAMENTO RELATIVAMENTE A: SISTEMI INFORMATICI; SISTEMI DI SICUREZZA INFORMATICA, APPLICAZIONI SW; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHÉ LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI; SISTEMI HARDWARE E SOFTWARE PER ELABORAZIONE DATI, RETI, COMUNICAZIONI, COMANDO E CONTROLLO PER I SETTORI: INDUSTRIA, BANCHE, ASSICURAZIONI, PUBBLICA AMMINISTRAZIONE, SERVIZI, TRASPORTI, UTILITIES, INFORMATION TECHNOLOGY; SOLUZIONI, SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI.
PROGETTAZIONE, INTEGRAZIONE, REALIZZAZIONE, ADEGUAMENTO E MANUTENZIONE DI SHELTER PER USO CIVILE; ALLESTIMENTO, ADEGUAMENTO E MANUTENZIONE DI ASSETTI PER COMUNICAZIONI STRATEGICHE INSTALLATI IN SHELTER E SU VEICOLI. PROGETTAZIONE, INTEGRAZIONE, MANUTENZIONE, INSTALLAZIONE E ASSISTENZA DI SISTEMI DI SICUREZZA INFORMATICA GESTITA (COMPRESI I SERVIZI DI SOC SECURITY OPERATION CENTER).
PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.

*IAF:33*
*IAF:19*
*IAF:28*

*RESEARCH AND DEVELOPMENT, DESIGN, REALIZATION, PRODUCTION, INSTALLATION, COMMISSIONING, MAINTENANCE, SUPPORT, SERVICE DELIVERY,TECHNICAL ADVICE AND TRAINING RELATING TO: INFORMATION SYSTEMS, COMPUTER SECURITY SYSTEMS, SW APPLICATIONS, CIVILIAN AND MILITARY CONTROL SYSTEMS, TRACKING SYSTEMS FOR CIVIL AND DEFENCE APPLICATIONS, AS WELL AS THEIR SUBSYSTEMS, EQUIPMENT AND DEVICES, HARDWARE AND SOFTWARE SYSTEMS FOR PROCESSING OF DATA, NETWORKS, COMMUNICATIONS, COMMAND AND CONTROL FOR THE SECTORS: INDUSTRY, BANKING, INSURANCE, PUBLIC ADMINISTRATION, SERVICES, TRANSPORTATION, UTILITIES, INFORMATION TECHNOLOGY, SOLUTIONS, SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS.*
*DESIGN, INTEGRATION, IMPLEMENTATION, ADJUSTMENT AND MAINTENANCE OF SHELTERS FOR CIVIL USE, PREPARATION, UPGRADING AND MAINTENANCE OF ASSETS FOR STRATEGIC COMMUNICATIONS INSTALLED IN SHELTERS AND ON VEHICLES.*
*DESIGN, INTEGRATION, MAINTENANCE, INSTALLATION AND SERVICING OF MANAGED INFORMATION SECURITY SYSTEMS (INCLUDING SOC - SECURITY INFORMATION CENTRE).*

IL PRESENTE CERTIFICATO DERIVA DAL CERTIFICATO OHS-169 CON DATA DI PRIMA EMISSIONE 20/12/2006

THIS CERTIFICATE IS DERIVED FROM

La validità del presente certificato è subordinata a sorveglianza periodica annuale / semestrale ed al riesame completo del sistema di gestione con periodicità triennale

*The validity of this certificate is dependent on an annual / six monthly audit and on a complete review, every three years, of the management system*

L'uso e la validità del presente certificato è soggetto al rispetto del documento RINA: Regolamento per la Certificazione dei Sistemi di Gestione della Sicurezza e Salute sul luogo di lavoro

*The use and validity of this certificate are subject to compliance with the RINA document: Rules for the Certification of Occupational Health and Safety Management Systems*

| | | | |
|---|---|---|---|
| Prima emissione<br>*First Issue* | 11.11.2016 | Data decisione di rinnovo<br>*Renewal decision date* | 09.11.2019 |
| Data scadenza<br>*Expiry Date* | 10.11.2022 | Data revisione<br>*Revision date* | 18.01.2021 |

Paolo Teramo

Italy Management System Certification Region, Senior Director

**RINA Services S.p.A.**
Via Corsica 12 - 16128 Genova Italy

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

## LEONARDO - SOCIETÀ PER AZIONI DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI LOCALITÀ PILL'E MATTA 09044 QUARTUCCIU (CA) ITALIA | INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, RELATIVAMENTE A SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI.<br>PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.<br>INSTALLATION, START-UP, MAINTENANCE, ASSISTANCE, SERVICE DELIVERY FOR SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS.<br>DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATIVE FOUNDATIONS, REINFORCED CONCRETE PRODUCTS, PREFABS AND RELATED TECHNOLOGICAL PLANTS, NECESSARY FOR START-UP. |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA E. MATTEI, 21 66013 CHIETI (CH) ITALIA | RICERCA E SVILUPPO, PROGETTAZIONE, INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, CONSULENZA TECNICA ED ADDESTRAMENTO RELATIVAMENTE A: SISTEMI INFORMATICI; SISTEMI DI SICUREZZA INFORMATICA, APPLICAZIONI SW; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHÉ LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI; SISTEMI HARDWARE E SOFTWARE PER ELABORAZIONE DATI, RETI, COMUNICAZIONI, COMANDO E CONTROLLO PER I SETTORI: INDUSTRIA, BANCHE, ASSICURAZIONI, PUBBLICA AMMINISTRAZIONE, SERVIZI, TRASPORTI, UTILITIES, INFORMATION TECHNOLOGY; SOLUZIONI, SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI.<br>INSTALLAZIONE E ASSISTENZA DI SISTEMI DI SICUREZZA INFORMATICA GESTITA (COMPRESI I SERVIZI DI SOC - SECURITY OPERATION CENTER).<br>RESEARCH AND DEVELOPMENT, DESIGN, REALIZATION, PRODUCTION, INSTALLATION, COMMISSIONING, MAINTENANCE, SUPPORT, SERVICE DELIVERY,TECHNICAL ADVICE AND TRAINING RELATING TO: INFORMATION SYSTEMS, COMPUTER SECURITY SYSTEMS, SW APPLICATIONS, CIVILIAN AND MILITARY CONTROL SYSTEMS, TRACKING SYSTEMS FOR CIVIL AND DEFENCE APPLICATIONS, AS WELL AS THEIR SUBSYSTEMS, EQUIPMENT AND DEVICES, HARDWARE AND SOFTWARE SYSTEMS FOR |

Data revisione
*Revision date* 18.01.2021

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| | PROCESSING OF DATA, NETWORKS, COMMUNICATIONS, COMMAND AND CONTROL FOR THE SECTORS: INDUSTRY, BANKING, INSURANCE, PUBLIC ADMINISTRATION, SERVICES, TRANSPORTATION, UTILITIES, INFORMATION TECHNOLOGY, SOLUTIONS, SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS. INSTALLATION AND SERVICING OF MANAGED INFORMATION SECURITY SYSTEMS (INCLUDING SOC - SECURITY INFORMATION CENTRE). |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA GIACOMO PUCCINI, 2 16154 GENOVA (GE) ITALIA | RICERCA E SVILUPPO, PROGETTAZIONE, REALIZZAZIONE, PRODUZIONE, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, CONSULENZA TECNICA ED ADDESTRAMENTO RELATIVAMENTE A: SISTEMI INFORMATICI; SISTEMI DI SICUREZZA INFORMATICA, APPLICAZIONI SW; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHÉ LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI; SISTEMI HARDWARE E SOFTWARE PER ELABORAZIONE DATI, RETI, COMUNICAZIONI, COMANDO E CONTROLLO PER I SETTORI: INDUSTRIA, BANCHE, ASSICURAZIONI, PUBBLICA AMMINISTRAZIONE, SERVIZI, TRASPORTI, UTILITIES, INFORMATION TECHNOLOGY; SOLUZIONI, SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI.<br>PROGETTAZIONE, INTEGRAZIONE, REALIZZAZIONE, ADEGUAMENTO E MANUTENZIONE DI SHELTER PER USO CIVILE; ALLESTIMENTO, ADEGUAMENTO E MANUTENZIONE DI ASSETTI PER COMUNICAZIONI STRATEGICHE INSTALLATI IN SHELTER E SU VEICOLI. PROGETTAZIONE, INTEGRAZIONE, MANUTENZIONE, INSTALLAZIONE E ASSISTENZA DI SISTEMI DI SICUREZZA INFORMATICA GESTITA (COMPRESI I SERVIZI DI SOC SECURITY OPERATION CENTER).<br>RESEARCH AND DEVELOPMENT, REALIZATION, PRODUCTION, INSTALLATION, COMMISSIONING, MAINTENANCE, SUPPORT, SERVICE |

Data revisione
*Revision date* 18.01.2021

FEDERAZIONE CISQ
www.cisq.com

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| | DELIVERY,TECHNICAL ADVICE AND TRAINING RELATING TO: INFORMATION SYSTEMS, COMPUTER SECURITY SYSTEMS, SW APPLICATIONS, CIVILIAN AND MILITARY CONTROL SYSTEMS, TRACKING SYSTEMS FOR CIVIL AND DEFENCE APPLICATIONS, AS WELL AS THEIR SUBSYSTEMS, EQUIPMENT AND DEVICES, HARDWARE AND SOFTWARE SYSTEMS FOR PROCESSING OF DATA, NETWORKS, COMMUNICATIONS, COMMAND AND CONTROL FOR THE SECTORS: INDUSTRY, BANKING, INSURANCE, PUBLIC ADMINISTRATION, SERVICES, TRANSPORTATION, UTILITIES, INFORMATION TECHNOLOGY, SOLUTIONS, SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS. DESIGN, INTEGRATION, IMPLEMENTATION, ADJUSTMENT AND MAINTENANCE OF SHELTERS FOR CIVIL USE, PREPARATION, UPGRADING AND MAINTENANCE OF ASSETS FOR STRATEGIC COMMUNICATIONS INSTALLED IN SHELTERS AND ON VEHICLES.<br>DESIGN, INTEGRATION, MAINTENANCE, INSTALLATION AND SERVICING OF MANAGED INFORMATION SECURITY SYSTEMS (INCLUDING SOC - SECURITY INFORMATION CENTRE). |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA GIOVANNI PALATUCCI, 1 07010 SASSARI (SS) ITALIA | INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, RELATIVAMENTE A SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI. PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.<br>INSTALLATION, START-UP, MAINTENANCE, ASSISTANCE, SERVICE DELIVERY FOR SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS. DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATIVE FOUNDATIONS, REINFORCED CONCRETE PRODUCTS, PREFABS AND RELATED TECHNOLOGICAL PLANTS, NECESSARY FOR START-UP. |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA LAURENTINA, 760 00143 ROMA (RM) ITALIA | RICERCA E SVILUPPO, PROGETTAZIONE, REALIZZAZIONE, PRODUZIONE, INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, CONSULENZA TECNICA ED ADDESTRAMENTO RELATIVAMENTE A: SISTEMI INFORMATICI; SISTEMI DI SICUREZZA INFORMATICA, APPLICAZIONI SW; SISTEMI DI CONTROLLO CIVILI E MILITARI; SISTEMI LOCALIZZAZIONE PER APPLICAZIONI CIVILI E DI DIFESA; NONCHÉ LORO SOTTOSISTEMI, APPARATI E DISPOSITIVI; SISTEMI HARDWARE E SOFTWARE PER ELABORAZIONE DATI, RETI, COMUNICAZIONI, COMANDO E CONTROLLO PER I SETTORI: INDUSTRIA, BANCHE, ASSICURAZIONI, PUBBLICA AMMINISTRAZIONE, SERVIZI, TRASPORTI, UTILITIES, INFORMATION TECHNOLOGY; SOLUZIONI, SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI. PROGETTAZIONE, INTEGRAZIONE, REALIZZAZIONE, ADEGUAMENTO E MANUTENZIONE DI SHELTER PER USO CIVILE; ALLESTIMENTO, ADEGUAMENTO E MANUTENZIONE DI ASSETTI PER COMUNICAZIONI STRATEGICHE INSTALLATI IN SHELTER E SU VEICOLI. PROGETTAZIONE, INTEGRAZIONE, MANUTENZIONE, INSTALLAZIONE E ASSISTENZA DI SISTEMI DI SICUREZZA INFORMATICA GESTITA (COMPRESI I SERVIZI DI SOC SECURITY OPERATION CENTER). PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| | MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.<br><br>PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO. |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Per informazioni sulla validità del certificato, visitare il sito www.rina.org

*For information concerning validity of the certificate, you can visit the site www.rina.org*

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA LORIEDO, 6 88046 LAMEZIA TERME (CZ) ITALIA | INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, RELATIVAMENTE A SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI.<br>PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.<br>INSTALLATION, START-UP, MAINTENANCE, ASSISTANCE, SERVICE DELIVERY FOR SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS.<br>DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATIVE FOUNDATIONS, REINFORCED CONCRETE PRODUCTS, PREFABS AND RELATED TECHNOLOGICAL PLANTS, NECESSARY FOR START-UP. |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CISQ is a member of IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
www.iqnet-certification.com

*IQNet, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world. IQNet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.*

# CERTIFICATO N. / *CERTIFICATE No.* OHS-2835

Altre unità operative coperte dal sistema di gestione di:
*Other operational units covered by the management system of:*

Per informazioni sulla validità del certificato, visitare il sito www.rina.org
*For information concerning validity of the certificate, you can visit the site www.rina.org*

## LEONARDO - SOCIETÀ PER AZIONI
## DIVISIONE CYBER SECURITY

Organizzazione operante secondo le prescrizioni del sistema di Gestione conforme alla Norma /
*Organization operating in accordance with the requirements of the Management System standard*

## ISO 45001:2018

| **Unità Operative/Operational units (Ragione sociale-Indirizzo Sito / Registered name - Site address)** | **Campi di attvità specifiche / Specific field(s) of activities** |
|---|---|
| LEONARDO - SOCIETÀ PER AZIONI VIA PEDRO ALVARES CABRAI, 14 87036 RENDE (CS) ITALIA | INSTALLAZIONE, MESSA IN ESERCIZIO, MANUTENZIONE, ASSISTENZA, EROGAZIONE SERVIZI, RELATIVAMENTE A SISTEMI, SOTTOSISTEMI, APPARATI PER CIFRATURA, TELECOMUNICAZIONE, RETI RADIOMOBILI PROFESSIONALI. PROGETTAZIONE E COSTRUZIONE DELLE STRUTTURE METALLICHE O IN CEMENTO ARMATO CON RELATIVE FONDAZIONI, MANUFATTI IN CEMENTO ARMATO, PREFABBRICATI ED IMPIANTI TECNOLOGICI CONNESSI, NECESSARI PER LA MESSA IN ESERCIZIO.<br>INSTALLATION, START-UP, MAINTENANCE, ASSISTANCE, SERVICE DELIVERY FOR SYSTEMS, SUBSYSTEMS, APPARATUS FOR ENCRYPTION, TELECOMMUNICATION, PROFESSIONAL RADIO MOBILE NETWORKS. DESIGN AND CONSTRUCTION OF METAL OR REINFORCED CONCRETE STRUCTURES WITH RELATIVE FOUNDATIONS, REINFORCED CONCRETE PRODUCTS, PREFABS AND RELATED TECHNOLOGICAL PLANTS, NECESSARY FOR START-UP. |

Data revisione
*Revision date* 18.01.2021

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO
SCR N° 003 F
Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
*Signatory of EA, IAF and ILAC Mutual Recognition Agreements*

FEDERAZIONE CISQ
www.cisq.com
CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale
*CISQ is the Italian Federation of management system Certification Bodies*



Form CERSISGE-01/2018

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della
Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1
dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO C

## OFFERTA ECONOMICA DEL FORNITORE – CATALOGO DEI SERVIZI

## Oggetto dell'Allegato

Il presente allegato è costituito dai seguenti annessi:

- Annesso 1: Offerta economica del Fornitore – Catalogo dei Servizi;
- Annesso 2: Offerta economica del Fornitore - dettagli del Listino 1.

## Listino 1

**Industry Standard**

| Tipologia | Elemento | CORE [Q] | RAM [GB] | vCPU [Q] | vRAM [GB] | Storage [GB] | Caratteristiche tecniche minime | Quantità | Canone Annuale | P X Q | Sconto % | Sconto € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IaaS Private (HA) | Blade Medium | 24 | 256 | | | | **Server features 2 socket Intel® Xeon® Scalable processor family, with up to 32 DIMMs (up to 6TB), PCIExpress® (PCIe)** | 45.321 | 11.083 € | 502.291.287 € | 55,00% | 6.095,65 € | 4.987 € | 226.031.079,06 € | 276.260.207,74 € |
| IaaS Private (HA) | Blade Large | 36 | 768 | | | | Server features 2 socket Intel® Xeon® Scalable processor family, with up to 32 DIMMs (up to 6TB), PCIExpress® (PCIe) 4.0 enabled I/O slots, and 2 high bandwidth Ethernet and Fiber Channel mezzanine card. All Ethernet interfaces are 10/25Gbps, fully redundant, with jumbo frame enabled end to end in the overall infrastructure. All FC interfaces are 32Gbps. Processore Intel 6354, 18 core, 3.0GHz, cache 39MB, 205W. Sistema operativo escluso | 7.558 | 15.922 € | 120.342.381 € | 49,50% | 7.881,15 € | 8.040 € | 60.772.902,26 € | 59.569.478,45 € |
| IaaS - Storage (HA) | Storage High Performance | | | | | 500 | SAN NVMe based, replicato intra-region, 170K IOPS per Storage Array | 18.145 | 721 € | 13.080.474 € | 49,50% | 356,84 € | 364 € | 6.605.639,28 € | 6.474.834,55 € |
| IaaS - Storage (HA) | Storage Standard Performance | | | | | 500 | SAN All Flash based, replicato intra-region, 130K IOPS per Storage Array | 27.217 | 395 € | 10.751.074 € | 49,50% | 195,53 € | 199 € | 5.429.292,56 € | 5.321.781,82 € |
| IaaS - Storage (HA) | NAS | | | | | 500 | NVMe based, replicato intra-region, 130K IOPS per Storage Array | 9.072 | 395 € | 3.583.691 € | 5,00% | 19,75 € | 375 € | 3.404.506,89 € | 179.184,57 € |
| IaaS - Storage (HA) | Object storage | | | | | 500 | Replicato inter-region | 18.145 | 395 € | 7.167.383 € | 49,50% | 195,53 € | 199 € | 3.619.528,37 € | 3.547.854,55 € |
| IaaS - Storage (HA) | Storage HP Encrypted | | | | | 500 | SAN NVMe based, replicato intra-region, crittografato a livello di singolo volume, 170K IOPS per Storage Array | 9.072 | 988 € | 8.959.229 € | 49,50% | 488,83 € | 499 € | 4.524.410,47 € | 4.434.818,18 € |
| IaaS - Storage (HA) | Storage SP Encrypted | | | | | 500 | SAN All Flash based, replicato intra-region, crittografato a livello di singolo volume, 130K IOPS per Storage Array | 9.072 | 652 € | 5.913.091 € | 49,50% | 322,63 € | 329 € | 2.986.110,91 € | 2.926.980,00 € |
| IaaS Shared (HA) | VM Tiny | | | 1 | 2 | 100 | Replica intra-region sincrona con duplicazione delle risorse sul secondario (0<RPO<1min, 0<RTO (IaaS)<30min); include i costi del backbone con latenza <5ms; Gestione hypervisor, over-commit 1:2 Sistema operativo escluso Infrastruttura basata su server Intel 6342, 24 core, cache 36MB, 230W | 127.055 | 544 € | 69.088.499 € | 49,50% | 269,17 € | 275 € | 34.889.691,89 € | 34.198.806,90 € |
| IaaS Shared (HA) | VM Small | | | 2 | 4 | 100 | | 95.296 | 1.077 € | 102.636.907 € | 60,00% | 646,22 € | 431 € | 41.054.762,66 € | 61.582.143,99 € |
| IaaS Shared (HA) | VM Medium | | | 4 | 8 | 100 | | 63.527 | 2.082 € | 132.234.893 € | 60,00% | 1.248,92 € | 833 € | 52.893.957,30 € | 79.340.935,96 € |
| IaaS Shared (HA) | VM Large | | | 8 | 16 | 100 | | 23.826 | 3.844 € | 91.580.381 € | 60,00% | 2.306,20 € | 1.537 € | 36.632.152,38 € | 54.948.228,57 € |
| IaaS Shared (HA) | VM X-Large | | | 16 | 32 | 100 | | 7.942 | 7.352 € | 58.393.299 € | 35,00% | 2.573,33 € | 4.779 € | 37.955.644,44 € | 20.437.654,70 € |
| IaaS Shared (HA) | Pool Small | | | 8 | 32 | | | 7.942 | 2.973 € | 23.608.717 € | 49,50% | 1.471,44 € | 1.501 € | 11.922.402,07 € | 11.686.314,90 € |
| IaaS Shared (HA) | Pool Medium | | | 16 | 64 | | | 7.942 | 5.435 € | 43.161.478 € | 49,50% | 2.690,08 € | 2.744 € | 21.796.546,37 € | 21.364.931,59 € |
| IaaS Shared (HA) | Pool Large | | | 32 | 128 | | | 3.966 | 10.529 € | 41.762.164 € | 55,00% | 5.790,98 € | 4.738 € | 18.792.973,58 € | 22.969.189,93 € |
| IaaS Shared (HA) | Pool XLarge | | | 64 | 256 | | | 992 | 19.310 € | 19.147.937 € | 45,00% | 8.689,62 € | 10.621 € | 10.531.365,29 € | 8.616.571,60 € |
| CaaS | Licensed - Medium | 24 | 256 | | | | HW IaaS Private, Tanzu Basic, Opzione Plus | 2.000 | 8.888 € | 17.779.519 € | 49,50% | 4.399,44 € | 4.488 € | 8.978.656,87 € | 8.800.861,68 € |
| CaaS | Licensed - Large | 36 | 768 | | | | HW IaaS Private, Tanzu Basic, Opzione Plus | 1.005 | 21.107 € | 21.220.071 € | 49,50% | 10.447,98 € | 10.659 € | 10.716.135,85 € | 10.503.935,14 € |
| CaaS | Open Source (vCPU/anno) | | | | | | Gestione ambienti kubernetes based | 2.000 | 889 € | 1.777.952 € | 49,50% | 439,94 € | 449 € | 897.865,69 € | 880.086,17 € |
| PaaS - DB | Mysql | | | 2 | | | Licenza inclusa (ultima/penultima versione certificata). Servizio gestito. | 18.886 | 1.900 € | 35.878.403 € | 20,00% | 379,94 € | 1.520 € | 28.702.722,57 € | 7.175.680,64 € |
| PaaS - DB | PostgreSQL | | | 2 | | | Licenza inclusa (ultima/penultima versione certificata). Servizio gestito. | 19.327 | 1.857 € | 35.888.786 € | 20,00% | 371,38 € | 1.486 € | 28.711.029,16 € | 7.177.757,29 € |
| PaaS - DB | SQL server | | | 2 | | | Licenza inclusa (ultima/penultima versione certificata). Servizio gestito. | 4.534 | 5.394 € | 24.456.162 € | 20,00% | 1.078,70 € | 4.315 € | 19.564.929,27 € | 4.891.232,32 € |
| PaaS - DB | Oracle dbms - Enterprise | | | 4 | 12 | | Servizio gestito (ultima/penultima versione certificata). Licenza Oracle Enterprise Edition inclusa. | 308 | 26.471 € | 8.146.849 € | 49,50% | 13.103,29 € | 13.368 € | 4.114.158,71 € | 4.032.690,22 € |
| PaaS - DB | Oracle dbms - Standard | | | 2 | 12 | | Servizio gestito (ultima/penultima versione certificata). Licenza Oracle Standard Edition inclusa. | 1.375 | 11.873 € | 16.321.653 € | 49,50% | 5.877,21 € | 5.996 € | 8.242.434,63 € | 8.079.218,10 € |
| PaaS - DB | MongoDB | | | 2 | | | Licenza inclusa (ultima/penultima versione certificata). Servizio gestito. | 1.559 | 6.261 € | 9.762.830 € | 49,50% | 3.099,16 € | 3.162 € | 4.930.229,09 € | 4.832.600,79 € |
| PaaS - DB | MariaDB | | | 2 | | | Licenza inclusa (ultima/penultima versione certificata). Servizio gestito. | 17.265 | 1.891 € | 32.655.483 € | 49,50% | 936,23 € | 955 € | 16.491.018,80 € | 16.164.463,97 € |
| PaaS - Big Data | Data Lake - 1TB | | | | | 1024 | HDFS - ridondanza 3 copie - 20K IOPS | 5.468 | 593 € | 3.240.000 € | 49,50% | 293,30 € | 299 € | 1.636.200,00 € | 1.603.800,00 € |
| PaaS - Big Data | Batch/Real time Processing - 1 Worker | | | 4 | 128 | | Apache Spark su processore fisico 26 core 2,70 Ghz con virtualization ratio 1:2 | 1.094 | 13.924 € | 15.228.000 € | 49,50% | 6.892,45 € | 7.032 € | 7.690.140,00 € | 7.537.860,00 € |
| PaaS - Big Data | Event Message - 1 Worker | | | 4 | 32 | | Apache Kafka su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 | 273 | 6.666 € | 1.822.500 € | 49,50% | 3.299,58 € | 3.366 € | 920.362,50 € | 902.137,50 € |
| PaaS - Big Data | Data Governance | | | | | | Portale self-service con catalogo e governance dei dati | 182 | 5.925 € | 1.080.000 € | 10,00% | 592,52 € | 5.333 € | 972.000,00 € | 108.000,00 € |
| Sistemi operativi | Windows Server STD CORE (2 core) | | | | | | Licenza Microsoft Server. Ultima release disponibile | 262.815 | 129 € | 34.032.715 € | 10,00% | 12,95 € | 117 € | 30.629.443,40 € | 3.403.271,49 € |
| Sistemi operativi | Red Hat per VM | | | | | | Licenza Red Hat per singola VM. Ultima release disponibile. | 100.899 | 604 € | 60.973.144 € | 10,00% | 60,43 € | 544 € | 54.875.829,95 € | 6.097.314,44 € |
| Sistemi operativi | Red Hat per Bare Metal | | | | | | Licenza per due socket. Ultima release disponibile. | 33.446 | 1.079 € | 36.092.276 € | 10,00% | 107,91 € | 971 € | 32.483.048,27 € | 3.609.227,59 € |
| Data Protection | Opzione DR | | | | | | Replica su altra region | 125.696.242 | 1 € | 105.557.636 € | 22,50% | 0,19 € | 1 € | 81.807.167,83 € | 23.750.468,08 € |
| Data Protection | Backup | | | | | 1.000 | Gestione delle policy in modalità self-managed; cifratura dei dati; ripristino granulare dei dati in modalità "a caldo e out-of-place"; seconda copia intra-region; GDPR compliant | - | 642 € | - € | 49,50% | 317,74 € | 324 € | - € | - € |
| Data Protection | Golden copy | | | | | 1.000 | Protezione antivirus, antimalware e anti-ramsonware proattivo; WORM copy; archiviazione in ambiente protetto privo di ogni accesso fisico e logico | - | 770 € | - € | 49,50% | 381,28 € | 389 € | - € | - € |
| Multicloud | CMP per server | | | | | | Portale self-service con catalogo dei servizi unificato; Governance; Dashboard personalizzabil; Capacity Planning; Compliance; Report di Cost Control e Capacity planning and Resource Usage; Performance Monitoring; Gestione finanziaria dell'IT | - | 148 € | - € | 49,50% | 73,32 € | 75 € | - € | - € |
| Security | Antivirus | | | | | | Prezzo per istanza | - | 829 € | - € | 49,50% | 410,52 € | 419 € | - € | - € |
| IaaS Shared | VM Tiny | | | 1 | 2 | 100 | Gestione hypervisor, over-commit 1:2. Sistema operativo escluso | - | 348 € | - € | 49,50% | 172,38 € | 176 € | - € | - € |
| IaaS Shared | VM Small | | | 2 | 4 | 100 | | - | 722 € | - € | 60,00% | 432,91 € | 289 € | - € | - € |
| IaaS Shared | VM Medium | | | 4 | 8 | 100 | | - | 1.415 € | - € | 60,00% | 848,97 € | 566 € | - € | - € |
| IaaS Shared | VM Large | | | 8 | 16 | 100 | | - | 2.629 € | - € | 60,00% | 1.577,40 € | 1.052 € | - € | - € |
| IaaS Shared | VM X-Large | | | 16 | 32 | 100 | | - | 5.046 € | - € | 35,00% | 1.766,18 € | 3.280 € | - € | - € |
| IaaS Shared | Pool Small | | | 8 | 32 | | | - | 1.951 € | - € | 49,50% | 965,85 € | 985 € | - € | - € |
| IaaS Shared | Pool Medium | | | 16 | 64 | | | - | 3.545 € | - € | 49,50% | 1.754,75 € | 1.790 € | - € | - € |
| IaaS Shared | Pool Large | | | 32 | 128 | | | - | 7.033 € | - € | 55,00% | 3.868,36 € | 3.165 € | - € | - € |
| IaaS Shared | Pool XLarge | | | 64 | 256 | | | - | 12.843 € | - € | 45,00% | 5.779,47 € | 7.064 € | - € | - € |
| IaaS Private | Blade Medium | 24 | 256 | | | | | - | 7.778 € | - € | 49,50% | 3.849,87 € | 3.928 € | - € | - € |
| IaaS Private | Blade Large | 36 | 768 | | | | | - | 11.172 € | - € | 49,50% | 5.529,97 € | 5.642 € | - € | - € |
| IaaS Shared (HA) | Pool - 1GB ram aggiuntivo | | | | 1 | | Risorsa aggiuntva per Pool IaaS shared | - | 64 € | - € | 49,50% | 31,68 € | 32 € | - € | - € |
| IaaS Shared (HA) | Pool - 1vCPU aggiuntiva | | | 1 | | | Risorsa aggiuntva per Pool IaaS shared | - | 126 € | - € | 49,50% | 62,37 € | 64 € | - € | - € |
| IaaS Shared | Pool - 1GB ram aggiuntivo | | | | 1 | | Risorsa aggiuntva per Pool IaaS shared | - | 45 € | - € | 49,50% | 22,28 € | 23 € | - € | - € |
| IaaS Shared | Pool - 1vCPU aggiuntiva | | | 1 | | | Risorsa aggiuntva per Pool IaaS shared | - | 88 € | - € | 49,50% | 43,56 € | 44 € | - € | - € |
| Connettività | Connessione dedicata 1 Gbps | | | | | | Tecnologia Gbe MPLS, profilo Silver 1000, TIR L2/L3 e outsourcing | - | 86.942 € | - € | 90,00% | 78.248,16 € | 8.694 € | - € | - € |
| **Tot Industry standard** | | | | | | | | | | **1.715.616.862 €** | **46,25%** | | | **922.206.338 €** | **793.410.523 €** |

## Listino 1

### Hybrid Cloud on PSN site

| Tipologia | Elemento | CORE | RAM | vCPU | vRAM | Storage | | Quantità | Canone Annuale | P X Q | Sconto % | Sconto € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Compute | Server 2-processore 26 core 768 GB RAM 24 TB Disco (o equivalente) | 52 | 768 | | | 48000 + 9600 | Azure Stack HCI + Azure ARC basato su Cluster SDDC basato su nodi processore fisico 26 core 2,70 Ghz, o equivalente<br>Storage Hyperconverged ibrido (6 x 1.6 TB SAS SSD Write-Intensive 12 x 4 TB 7.2K SAS)<br>Infrastruttura di rete ethernet 10/25 Gbps<br>incluse Licenze di virtualizzazione (Compute, Network & Storage)<br>Gestione sistemistica e monitoraggio di sicurezza fino all'hypervisor e integrazione | 3.089 | 57.883 € | 178.790.938 € | 7,00% | 4.052 € | 53.832 € | 166.275.572 € | 12.515.366 € |
| Policy | Server | | | | | | Policy per server | 33.393 | 86 € | 2.857.930 € | 7,00% | 6 € | 80 € | 2.657.875 € | 200.055 € |
| Kubernetes | vCPU | | | 1 | | | | 53.428 | 29 € | 1.545.568 € | 7,00% | 2 € | 27 € | 1.437.379 € | 108.190 € |
| SQL Data services | vCPU | | | 1 | | | Postgres o Sql server | 10.018 | 2.213 € | 22.168.389 € | 7,00% | 155 € | 2.058 € | 20.616.602 € | 1.551.787 € |
| Monitoring | GB | | | | | | GB di log analizzati al giorno | 14.609 | 1.322 € | 19.319.902 € | 7,00% | 93 € | 1.230 € | 17.967.509 € | 1.352.393 € |
| **TOT Hybrid Cloud on PSN site** | | | | | | | | | | **224.682.728 €** | **7,00%** | | | **208.954.937 €** | **15.727.791 €** |

### Secure Public Cloud (1)

| Tipologia | Elemento | | | | | | | Quantità | Canone Annuale | P X Q | Sconto % | Sconto € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Progetto Cloud 1** | | | | | | | | 694 | 550.531 € | 382.290.699 € | 7,00% | 38.537 € | 511.994 € | 355.530.350 € | 26.760.349 € |
| **Progetto Cloud 2** | | | | | | | | 477 | 342.591 € | 163.553.812 € | 7,00% | 23.981 € | 318.610 € | 152.105.046 € | 11.448.767 € |
| **Tot Secure Public Cloud** | | | | | | | | | | **545.844.511 €** | **7,00%** | | | **507.635.395 €** | **38.209.116 €** |

### Public Cloud PSN managed (2)

| Tipologia | Elemento | | | | | | | Quantità | Canone Annuale | P X Q | Sconto % | Sconto € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CLUSTER 1** | | | | | | | | 67 | 590.778 € | 39.774.566 € | 30,00% | 177.233 | 413.545 € | 27.842.196 € | 11.932.370 € |
| **CLUSTER 2** | | | | | | | | 96 | 490.747 € | 46.880.960 € | 30,00% | 147.224 | 343.523 € | 32.816.672 € | 14.064.288 € |
| **CLUSTER 3** | | | | | | | | 96 | 500.359 € | 47.799.157 € | 30,00% | 150.108 | 350.251 € | 33.459.410 € | 14.339.747 € |
| **CLUSTER 4** | | | | | | | | 96 | 1.113.436 € | 106.366.305 € | 30,00% | 334.031 | 779.405 € | 74.456.413 € | 31.909.891 € |
| **CLUSTER 5*** | | | | | | | | 91 | 918.730 € | 83.586.713 € | 30,00% | 275.619 | 643.111 € | 58.510.699 € | 25.076.014 € |
| **Tot Public Cloud PSN managed** | | | | | | | | | | **324.407.700 €** | **30,00%** | | | **227.085.390 €** | **97.322.310 €** |
| **TOTALE LISTINO 1** | | | | | | | | | | **2.810.551.800 €** | **33,61%** | | | **1.865.882.060 €** | **944.669.740 €** |

(1) per I dettagli dei progetti fare riferimento al documento "listino", allegato n

(2) per I dettagli dei Cluster fare riferimento al documento "listino", allegato n

*il valore totale del Cluster 5 è stato corretto rispetto al listino originario al fine di correggere il calcolo

## Listino 2

### Industry Standard

| Tipologia | Elemento | CORE [Q] | RAM [GB] | vCPU [Q] | vRAM [GB] | Storage [GB] | Caratteristiche tecniche minime | Quantità | Canone Annuale | P X Q | Sconto % | Sconto € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Housing | Rack | | | | | | 1.75 mq, 3.5kw di energia inclusa, prossimità, cablaggi (16 fibra + 2 rame), suite | 4.774 | 16.693 € | 79.692.584 € | 7,91% | 1.320 € | 15.374 € | 73.392.752 € | 6.299.833 € |
| Hosting | Server (1RU) | 16 | 64 | | | 2.700 | Server dedicato ospitato all'interno di un rack condiviso. Sistema operativo escluso. Processore: Intel Gold 6334, 8 core, 3.6GHz, cache 18MB, 165W | 47.253 | 10.674 € | 504.374.026 € | 54,99% | 5.870 € | 4.804 € | 227.017.828 € | 277.356.198 € |
| Hosting | Server su rack dedicato (1RU) | 16 | 64 | | | 2.700 | Server e rack dedicato. Sistema operativo escluso. Processore Intel Gold 6334, 8 core, 3.6GHz, cache 18MB, 165W | 11.816 | 13.801 € | 163.069.400 € | 53,22% | 7.344 € | 6.456 € | 76.287.267 € | 86.782.132 € |
| Hosting - Storage | Storage High Performance | | | | | 500 | SAN NVMe based, 170K IOPS per Storage Array | 6.968 | 360 € | 2.511.475 € | 61,67% | 222 € | 138 € | 962.651 € | 1.548.824 € |
| Hosting - Storage | Storage Standard Performance | | | | | 500 | SAN All Flash based, 130K IOPS per Storage Array | 10.451 | 198 € | 2.064.226 € | 30,05% | 59 € | 138 € | 1.443.977 € | 620.250 € |
| Hosting - Storage | NAS | | | | | 500 | NVMe based, 130K IOPS per Storage Array | 3.484 | 198 € | 688.075 € | 30,05% | 59 € | 138 € | 481.326 € | 206.750 € |
| Hosting - Storage | Object storage | | | | | 500 | | 6.968 | 198 € | 1.376.151 € | 18,16% | 36 € | 162 € | 1.126.182 € | 249.969 € |
| Hosting - Storage | Storage HP Encrypted | | | | | 500 | SAN NVMe based, crittografato a livello di singolo volume, 170K IOPS per Storage Array | 3.484 | 494 € | 1.720.189 € | 72,02% | 356 € | 138 € | 481.326 € | 1.238.863 € |
| Hosting - Storage | Storage SP Encrypted | | | | | 500 | SAN All Flash based, crittografato a livello di singolo volume, 130K IOPS per Storage Array | 3.484 | 326 € | 1.135.325 € | 57,60% | 188 € | 138 € | 481.326 € | 653.999 € |
| Housing | Potenza elettrica aggiuntiva (pacchetto da 1kW di targa) | | | | | | | - | 1.384 € | - € | 0,00% | - € | 1.384 € | - € | - € |
| Housing | Rilancio connettività (fibra monomodale) | | | | | | Rilancio in fibra intra-Data Center | - | 183 € | - € | 40,50% | 74 € | 109 € | - € | - € |
| Housing | IP Pubblico singolo | | | | | | | - | 40 € | - € | 40,50% | 16 € | 24 € | - € | - € |
| Housing | IP Pubblici /29 (8 indirizzi) | | | | | | | - | 110 € | - € | 40,50% | 45 € | 65 € | - € | - € |
| Housing | Cage | | | | | | Serratura sul rack del cliente | - | 570 € | - € | 40,50% | 231 € | 339 € | - € | - € |
| Housing | Housing router in sala TLC | | | | | | Housing di un router cliente per connettività esterna dedicata | - | 3.534 € | - € | 40,50% | 1.431 € | 2.103 € | - € | - € |
| Housing | Moving server | | | | | | Moving di un server da sede cliente al Data Center del PSN | - | 4.000 € | - € | 40,50% | 1.620 € | 2.380 € | - € | - € |
| PaaS - AI | AI Platform - 1 Worker - 1 GPU | | | 8 | 64 | | Spark/Tensorflow/Keras/scikit processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 - Nvidia A100 dedicata | 729 | 24.886 € | 18.144.000 € | 40,50% | 10.079 € | 14.807 € | 10.795.680 € | 7.348.320 € |
| PaaS - AI | Semantic Knowledge Search - 1 Worker | | | 8 | 32 | 2046 | ElasticSearch su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 - Disco SSD | 1.094 | 4.740 € | 5.184.000 € | 40,50% | 1.920 € | 2.820 € | 3.084.480 € | 2.099.520 € |
| PaaS - AI | Text Analytics /NLP - 1 Worker | | | 8 | 32 | | Analisi linguistica con entity recognition, sentiment analysis, NER su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 | 365 | 7.643 € | 2.786.400 € | 40,50% | 3.096 € | 4.548 € | 1.657.908 € | 1.128.492 € |
| PaaS - AI | Audio Analytics - 1 flusso audio H24 X 365G | | | | | | Analisi audio per speech to text, text to speech,speaker verification, speaker identification, anomaly detection | 911 | 4.266 € | 3.888.000 € | 40,50% | 1.728 € | 2.538 € | 2.313.360 € | 1.574.640 € |
| PaaS - AI | Video Analytics - 1 flusso video H24 X 365G | | | | | | Analisi video per object recognition, object tracking, face recognition, crowd counting | 1.823 | 12.591 € | 22.950.000 € | 40,50% | 5.099 € | 7.492 € | 13.655.250 € | 9.294.750 € |
| PaaS - Spid Enabling & Profiling | Spid Enabling & Profiling 100 Utenti | | | | | | | 1.823 | 9.777 € | 17.820.000 € | 40,50% | 3.959 € | 5.817 € | 10.602.900 € | 7.217.100 € |
| **Tot Industry Standard** | | | | | | | | | | **827.403.852 €** | **48,78%** | | | **423.784.212 €** | **403.619.640 €** |

| Tipologia Priorità 2 | Figura | Descrizione | Quantità | Canone | P X Q | Sconto % | Sconto unitario € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|
| Figura professionale | Project Manager (tariffa giorno/persona) | Rearch&Replat, Profess Serv | 103.167 | 465 € | 47.972.558 € | 20,04% | 93 € | 372 € | 38.357.418 € | 9.615.140 € |
| Figura professionale | Cloud Application Architect (tariffa giorno/persona) | Rearch&Replat, Profess Serv | 55.297 | 651 € | 35.998.126 € | 40,50% | 264 € | 387 € | 21.418.885 € | 14.579.241 € |
| Figura professionale | UX Designer (tariffa giorno/persona) | Rearch&Replat | 46.015 | 372 € | 17.117.580 € | 20,04% | 75 € | 297 € | 13.686.703 € | 3.430.877 € |
| Figura professionale | Business Analyst (tariffa giorno/persona) | Rearch&Replat | 46.015 | 372 € | 17.117.580 € | 20,04% | 75 € | 297 € | 13.686.703 € | 3.430.877 € |
| Figura professionale | DevOps Expert (tariffa giorno/persona) | Rearch&Replat | 92.029 | 391 € | 35.983.339 € | 20,04% | 78 € | 313 € | 28.771.198 € | 7.212.141 € |
| Figura professionale | Database Specialist and Administrator (tariffa giorno/persona) | Rearch&Replat, IT Infrastructur-service operation | 78.854 | 419 € | 33.039.972 € | 40,50% | 170 € | 249 € | 19.658.783 € | 13.381.189 € |
| Business & Culture Enablement F | Developer (Cloud/Mobile/Front-End Developer) (tariffa giorno/persona) | Rearch&Replat, Business&Culture Enablement | 206.005 | 233 € | 47.999.254 € | 20,04% | 47 € | 186 € | 38.378.763 € | 9.620.490 € |
| Figura professionale | System Integrator & Testing Specialist (tariffa giorno/persona) | | - | 353 € | - € | 20,04% | 71 € | 282 € | - € | - € |
| Figura professionale | System and Network Administrator (tariffa giorno/persona) | Rearch&Replat, IT Infrastructur-service operation | 136.154 | 372 € | 50.649.266 € | 20,04% | 75 € | 297 € | 40.497.634 € | 10.151.632 € |
| Figura professionale | Cloud Application Specialist (tariffa giorno/persona) | Rearch&Replat, Profess Serv | 125.286 | 530 € | 66.401.610 € | 40,50% | 215 € | 315 € | 39.508.958 € | 26.892.652 € |
| Figura professionale | Cloud Security Specialist (tariffa giorno/persona) | Rearch&Replat, IT Infrastructur-service operation | 77.110 | 419 € | 32.309.056 € | 40,50% | 170 € | 249 € | 19.223.889 € | 13.085.168 € |
| Figura professionale | Enterprise Architect (tariffa giorno/persona) | Rearch&Replat | 46.015 | 698 € | 32.118.470 € | 40,50% | 283 € | 415 € | 19.110.490 € | 13.007.980 € |
| Figura professionale | Security Principal (tariffa giorno/persona) | Profess Serv | 9.282 | 651 € | 6.042.361 € | 20,04% | 130 € | 521 € | 4.831.291 € | 1.211.070 € |
| Figura professionale | Senior Information Security Consultant (tariffa giorno/persona) | Profess Serv | 9.282 | 530 € | 4.919.280 € | 20,04% | 106 € | 424 € | 3.933.309 € | 985.971 € |
| Figura professionale | Junior Information Security Consultant (tariffa giorno/persona) | Profess Serv | 14.851 | 372 € | 5.524.593 € | 20,04% | 75 € | 297 € | 4.417.299 € | 1.107.294 € |
| Figura professionale | Security Solution Architect (tariffa giorno/persona) | Profess Serv | 18.563 | 530 € | 9.838.560 € | 20,04% | 106 € | 424 € | 7.866.617 € | 1.971.943 € |
| Figura professionale | Senior Security Auditor/Analyst (tariffa giorno/persona) | Profess Serv | 40.839 | 558 € | 22.788.109 € | 20,04% | 112 € | 446 € | 18.220.688 € | 4.567.421 € |
| Figura professionale | Junior Security Analyst (tariffa giorno/persona) | Profess Serv | 18.563 | 353 € | 6.552.852 € | 20,04% | 71 € | 282 € | 5.239.464 € | 1.313.388 € |
| Figura professionale | Senior Penetration Tester (tariffa giorno/persona) | Profess Serv | 7.426 | 465 € | 3.452.871 € | 20,04% | 93 € | 372 € | 2.760.812 € | 692.059 € |
| Figura professionale | Junior Penetration Tester (tariffa giorno/persona) | Profess Serv | 11.138 | 326 € | 3.630.920 € | 20,04% | 65 € | 261 € | 2.903.175 € | 727.745 € |
| Figura professionale | Forensic Expert (tariffa giorno/persona) | Profess Serv | 7.426 | 465 € | 3.452.871 € | 20,04% | 93 € | 372 € | 2.760.812 € | 692.059 € |
| Figura professionale | Data Protection Specialist (tariffa giorno/persona) | Profess Serv | 12.994 | 465 € | 6.042.175 € | 20,04% | 93 € | 372 € | 4.831.141 € | 1.211.033 € |
| Figura professionale | Systems Architect (tariffa giorno/persona) | Profess Serv | 8.283 | 605 € | 5.011.440 € | 20,04% | 121 € | 484 € | 4.006.997 € | 1.004.443 € |
| Business & Culture Enablement F | Product/Network/Technical Specialist (tariffa giorno/persona) | Profess Serv | 84.530 | 419 € | 35.418.040 € | 20,04% | 84 € | 335 € | 28.319.203 € | 7.098.838 € |
| Business & Culture Enablement F | Educational Designer/Tutoring (tariffa giorno/persona) | Business & Culture Enablement Figura professionale | 14.632 | 372 € | 5.442.950 € | 20,04% | 75 € | 297 € | 4.352.020 € | 1.090.931 € |
| Business & Culture Enablement | Costo adesione al servizio per Amministrazione | Business & Culture Enablement Figura professionale | 70 | 38.588 € | 2.701.160 € | 40,50% | 15.628 € | 22.960 € | 1.607.190 € | 1.093.970 € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 0 a 1.000 | Business & Culture Enablement Figura professionale | 2.593 | 226 € | 587.081 € | 0,00% | - € | 226 € | 587.081 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 1.001 a 5.000 | Business & Culture Enablement Figura professionale | 239 | 453 € | 108.384 € | 0,00% | - € | 453 € | 108.384 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 5.001 a 10.000 | Business & Culture Enablement Figura professionale | 239 | 679 € | 162.576 € | 0,00% | - € | 679 € | 162.576 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 10.001 a 20.000 | Business & Culture Enablement Figura professionale | 12 | 1.019 € | 12.193 € | 0,00% | - € | 1.019 € | 12.193 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 20.001 a 50.000 | Business & Culture Enablement Figura professionale | 12 | 1.585 € | 18.967 € | 0,00% | - € | 1.585 € | 18.967 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 50.001 a 100.000 | Business & Culture Enablement Figura professionale | 12 | 2.377 € | 28.451 € | 0,00% | - € | 2.377 € | 28.451 € | - € |
| Business & Culture Enablement | Canone settimanale per fascia utenti da 100.001 a 150.000 | Business & Culture Enablement Figura professionale | 12 | 3.170 € | 37.934 € | 0,00% | - € | 3.170 € | 37.934 € | - € |
| Business & Culture Enablement | Corso bassa interattività | Business & Culture Enablement Figura professionale | 159 | 3.483 € | 554.304 € | 45,00% | 1.567 € | 1.915 € | 304.867 € | 249.437 € |
| Business & Culture Enablement | Corso media interattività | Business & Culture Enablement Figura professionale | 159 | 4.937 € | 785.761 € | 45,00% | 2.222 € | 2.715 € | 432.168 € | 353.592 € |
| Business & Culture Enablement | Corso alta interattività | Business & Culture Enablement Figura professionale | 159 | 6.503 € | 1.035.075 € | 45,00% | 2.926 € | 3.577 € | 569.291 € | 465.784 € |
| Business & Culture Enablement | A catalogo | Business & Culture Enablement Figura professionale | 159 | 5.500 € | 875.402 € | 0,00% | - € | 5.500 € | 875.402 € | - € |
| **Tot Figure Professionali** | | | | | **541.731.124 €** | **27,73%** | | | **391.486.759,15 €** | **150.244.364,36 €** |
| **TOTALE LISTINO 2** | | | | | **1.369.134.975 €** | **40,45%** | | | **815.270.971 €** | **553.864.004,16** |

## Listino 3

| Tipologia MIGRAZIONE | Figura | Attività | Quantità | Canone | P X Q | Sconto % | Sconto unitario € | Canone Annuale Scontato | Pscontato X Q | Sconto totale |
|---|---|---|---|---|---|---|---|---|---|---|
| Figura professionale | Cloud Application Architect (tariffa giorno/persona) | Migrazione | 50.407 | 651 € | 32.815.083 € | 40,50% | 264 € | 387 € | 19.524.974 € | 13.290.108 € |
| Figura professionale | Database Specialist and Administrator (tariffa giorno/persona) | Migrazione | 75.611 | 419 € | 31.680.921 € | 40,50% | 170 € | 249 € | 18.850.148 € | 12.830.773 € |
| Figura professionale | System Integrator & Testing Specialist (tariffa giorno/persona) | Migrazione | 151.222 | 353 € | 53.381.217 € | 40,50% | 143 € | 210 € | 31.761.824 € | 21.619.393 € |
| Figura professionale | Cloud Application Specialist (tariffa giorno/persona) | Migrazione | 100.814 | 530 € | 53.431.625 € | 40,50% | 215 € | 315 € | 31.791.817 € | 21.639.808 € |
| Figura professionale | Cloud Security Specialist (tariffa giorno/persona) | Migrazione | 75.611 | 419 € | 31.680.921 € | 40,50% | 170 € | 249 € | 18.850.148 € | 12.830.773 € |
| Figura professionale | Enterprise Architect (tariffa giorno/persona) | Migrazione | 50.407 | 698 € | 35.184.221 € | 40,50% | 283 € | 415 € | 20.934.611 € | 14.249.609 € |
| **Totale LISTINO 3** | | | | | **238.173.987 €** | **40,50%** | | | **141.713.522 €** | **96.460.465 €** |

**SECURE PUBLIC CLOUD** — **Microsoft Azure West Europe**

| Macrotipologia | Tipo | Tipologia | Tipo | Quantità | Listino PSN | Indicazione Servizio Public Cloud di riferimento |
|---|---|---|---|---|---|---|
| Compute & Network | Compute (Production) Riservate 3 anni | VM "convenzionali" | c1r2 | 3 | 228,55 € | F1s |
| | | | c1r4 | 5 | 286,47 € | F2s v2 |
| | | | c2r4 | 6 | 286,47 € | F2s v2 |
| | | | c2r8 | 8 | 426,57 € | D2sv3 |
| | | | c2r16 | 10 | 468,21 € | E2s v4 |
| | | | c4r8 | 10 | 567,53 € | F4s v2 |
| | | | c4r16 | 11 | 853,45 € | D4sv3 |
| | | | c4r32 | 10 | 936,42 € | E4s v4 |
| | | | c8r16 | 9 | 1.134,75 € | F8s v2 |
| | | | c8r32 | 7 | 1.706,91 € | D8sv3 |
| | | | c8r64 | 6 | 1.872,85 € | E8s v4 |
| | | | c16r32 | 5 | 2.269,50 € | F16s v2 |
| | | | c16r64 | 4 | 3.413,51 € | D16s v3 |
| | | VM Confidential | c1r4 | 3 | 651,21 € | DC1s v2 |
| | | | c2r8 | 6 | 1.302,81 € | DC2s v2 |
| | | | c4r16 | 11 | 2.605,23 € | DC4s v2 |
| | | | c8r32 | 7 | 5.210,98 € | Dc8s V2 |
| | | CaaS convenzionale | c4r16 | 8 | 853,45 € | D4sv3 |
| | | CaaS Confidential | c4r16 | 8 | 2.605,23 € | DC4s v2 |
| | | MS SQL server convenzionale | serverless 4-core 500 GB con | 1 | 18.516,39 € | SQL MI BC LRS - 512GB con Licenza - 3Y RI |
| | | PostgreSQL convenzionale | 4-core 500 GB con licenza | 1 | 4.113,37 € | Azure Database for PostgreSQL - 500GB |
| | | Machine Learning | c4r16 | 4 | 861,65 € | Azure machine learning D4sv3 |
| | | Artificial Intelligence - Speech-to-Text | 300 Hrs/month | 1 | 3.310,88 € | Azure Cognitive Services - AAA-92197 |
| | | Web App -aaS | c4r8 | 3 | 9.796,52 € | App Service Windows - Isolated v2 (I3) RI 3Y |
| | Compute a consumo(Altri ambienti) | VM "convenzionali" | c1r2 | 1 | 437,88 € | F1s |
| | | | c1r4 | 1 | 759,63 € | F2s v2 |
| | | | c2r4 | 1 | 759,63 € | F2s v2 |
| | | | c2r8 | 1 | 923,30 € | D2sv3 |
| | | | c2r16 | 1 | 1.171,95 € | E2s v4 |
| | | | c4r8 | 1 | 1.499,22 € | F4s v2 |
| | | | c4r16 | 1 | 1.846,60 € | D4sv3 |
| | | | c4r32 | 1 | 2.343,90 € | E4s v4 |
| | | | c8r16 | 1 | 2.989,29 € | F8s v2 |
| | | | c8r32 | 1 | 3.702,33 € | D8sv3 |
| | | | c8r64 | 1 | 4.686,88 € | E8s v4 |
| | | | c16r32 | 1 | 5.987,72 € | F16s v2 |
| | | | c16r64 | 1 | 7.404,67 € | D16s v3 |
| | | VM "confidential" | c1r4 | 1 | 1.039,38 € | DC1s v2 |
| | | | c2r8 | 1 | 2.066,24 € | DC2s v2 |
| | | | c4r16 | 1 | 4.156,28 € | DC4s v2 |
| | | | c8r32 | 1 | 8.310,06 € | Dc8s V2 |
| | Storage | Managed Disks | dischi SSD Standard (128 GB) | 138 | 101,43 € | E10 (AAD-36603) |
| | Storage | Managed Disks | dischi SSD Premium (128 GB) | 138 | 228,91 € | P10 (AAD-18125) |
| | | Connection Gateway | ore di servizio | 8760 | 0,56 € | ExpressRoute Gateway - ErGw2AZ - Gateway |

**SECURE PUBLIC CLOUD** — **Microsoft Azure West Europe**

| Macrotipologia | Tipo | Tipologia | Tipo | Quantità | Listino PSN | Indicazione Servizio Public Cloud di riferimento |
|---|---|---|---|---|---|---|
| | Network | Bandwidth (GB/anno) | GB per anno | 24000 | 0,02 € | ExpressRoute - Metered Data Data Transfer Out - Zone 1 |
| | | Speed (Gbs) | Giorni di accensione | 365 | 24,75 € | ExpressRoute - Standard - Metered Data - 2 Gbps Circuit - Zone 1 |
| | | Bandwidth Internet (TB/anno) | TB annui | 12 | 77,00 € | Bandwidth - Routing Preference: Microsoft Global network - Data Transfer Out - Zone 1 |
| Public Cloud Security & Backup | Defense in Depth | XDR per Servers | istanze | 138 | 154,15 € | Azure Defender for servers - Standard - Nodes |
| | | XDR per SQL | istanze | 6 | 158,41 € | Azure Defender for SQL - Standard Node - Istanze/mese |
| | | XDR per Storage | 1M Transazioni Standard per | 140,5 | 21,16 € | Azure Defender for Storage - Standard Transactions |
| | | XDR per Kubernetes | vCore | 64 | 20,75 € | Azure Defender for Kubernetes - Standard Cores |
| | | XDR per container registry | 100 immagini standard | 1 | 25,53 € | Azure Defender for container registries - Standard Images |
| | | XDR per Key Vault | 1M Transazioni Standard | 2 | 17,59 € | Azure Defender for Key Vault - Standard Transactions |
| | SIEM | SIEM service | GB per giorno | 31,74 | 823,74 € | Sentinel - Analysis - EU West (stima per 40 GB al giorno) |
| | | SIEM Data Ingestion | GB per giorno | 31,74 | 789,43 € | Log Analytics - Data Ingestion - EU West |
| | | SIEM Data retention (6 mesi) | GB per giorno | 31,74 | 125,23 € | 3 mesi gratuiti di retention per Sentinel |
| | Monitor | Monitor VM Data ingestion | GB per giorno | 31,74 | 789,43 € | Log Analytics - Data Ingestion - EU West |
| | | Monitor Data retention (1 mesi) | GB per giorno | 1 | - € | 1 mese gratuito di retention per LogAnalytics |
| | Firewall | Deployment | Istanze | 1 | 13.490,95 € | Azure FW Premium (AAF-69092) |
| | | Data managed | TB mese | 6 | 173,06 € | Azure FW Premium - Data Processed (6TB mese) (AAF-69161) |
| | Cloud Backup | Istanze Protette | Numero VM | 138 | 106,19 € | |
| | | Storage occupato | GB | 35328 | 0,25 € | |
| PSN Security & Backup | Professional Services | 10 giorni/mese (Security Posture, Policy Verification) | | | | |
| | Key Vault | Managed HSM and AKV operations (HSM on premise) | | | | |
| | Backup on premise | Storage | | | | |
| | Addictional Security | | | | | |
| | | | | **TOTALE Progetto Cloud 1** | **511.994** | |

**SECURE PUBLIC CLOUD** **GPC**

| Macrotipologia | Tipo | Tipologia | Tipo | Quantità | Listino PSN | Indicazione Servizio Public Cloud di riferimento |
|---|---|---|---|---|---|---|
| Compute & Network | Compute (Production) riservate a 3 anni | VM "convenzionali", | c1r4 | 4 | 177,93 € | n1-standard-1 |
| | | | c2r4 | 5 | 125,50 € | e2-medium |
| | | | c2r8 | 6 | 251,00 € | e2-standard-2 |
| | | | c2r16 | 7 | 338,62 € | e2-highmem-2 |
| | | | c4r16 | 9 | 695,21 € | c2-standard-4 |
| | | | c4r32 | 8 | 677,24 € | e2-highmem-4 |
| | | | c8r32 | 7 | 1.390,54 € | c2-standard-8 |
| | | | c8r64 | 6 | 1.354,61 € | e2-highmem-8 |
| | | | c16r64 | 4 | 2.780,95 € | c2-standard-16 |
| | | VM Confidential | c1r4 | 3 | 241,74 € | n1-standard-1 |
| | | | c2r8 | 6 | 378,64 € | e2-standard-2 |
| | | | c4r16 | 9 | 982,87 € | n2-standard-4 |
| | | | c8r32 | 6 | 1.776,44 € | n2d-standard-8 |
| | | CaaS convenzionale | c4r16 | 6 | 1.293,87 € | n2-standard-4 |
| | | CaaS Confidential | c4r16 | 6 | 1.549,15 € | n2-standard-4 |
| | | PostgreSQL convenzionale | 4-core 500 GB con licenza | 1 | 1.862,48 € | db-standard-4 |
| | Compute a consumo(Altri ambienti) | VM "convenzionali" | c1r4 | 1 | 276,79 € | db-standard-4 |
| | | | c2r4 | 1 | 278,99 € | c2-standard-4 |
| | | | c2r8 | 1 | 557,85 € | Speech-to-Text |
| | | | c4r16 | 1 | 752,52 € | n1-standard-1 |
| | | | c4r32 | 1 | 1.505,04 € | e2-medium |
| | | | c8r32 | 1 | 2.263,55 € | e2-highmem-2 |
| | | | c16r64 | 1 | 4.462,69 € | e2-highmem-4 |
| | | VM "confidential" | c2r8 | 1 | 2.251,33 € | n2d-standard-8 |
| | | | c4r16 | 1 | 3.010,20 € | e2-highmem-8 |
| | Storage | Managed Disks | dischi SSD Standard (128 GB) | 280 | 55,57 € | |
| | Network | Networking Cloud Load Balancing HTTPS External Regional Forwarding Rule Europe | rule (per day per project) | 5 | 89,21 € | 5 LB |
| | | Cloud Interconnect for MPS - 10Gbps Pa | circuiti | 1 | 18.287,53 € | 1 |
| | | Cloud Interconnect for MPS - 10Gbps Partner circuit | vlan attachment | 2 | 446,04 € | 2 vlan attachment |
| | | Egress to EMEA | gigabyte | 12000 | 0,18 € | 1TB mese |
| Public Cloud Security & Backup | Web Protection | Policy | number policy | 25 | 52,86 € | Cloud Armon Policies |
| | | Rules | number rules | 25 | 10,57 € | Cloud Armor rules |
| | | Incoming Request | milion request | 5 | 7,93 € | Cloud Armor incoming request |
| | | Chapcha | 1000 requests | 4000 | 0,01 € | recapcha |
| | | Container Analysis | scanned image | 150 | 2,75 € | |
| | SIEM | User Monitoring | user | 1000 | 37,68 € | Chronicle |
| | | Daily Data Volume | 20 gigabyte | 5 | 5.689,95 € | Security Command Center Premium Tier |
| | Data Loss Prevention | Storage Bytes Inspected (fino a 51,200 G | gigabyte | 50 | 9,85 € | |
| | | Storage Bytes Inspected (51,200 GiB - 51 | gigabyte | 450 | 7,39 € | |
| | | Storage Bytes Inspected (>512,000 gibib | gigabyte | 4550 | 5,91 € | |
| | | Storage Bytes Transformed (fino a 51,20 | gigabyte | 50 | 9,85 € | |

**SECURE PUBLIC CLOUD**

| | | | | | | **GPC** |
|---|---|---|---|---|---|---|
| **Macrotipologia** | **Tipo** | **Tipologia** | **Tipo** | **Quantità** | **Listino PSN** | **Indicazione Servizio Public Cloud di riferimento** |
| | | Storage Bytes Transformed (>512,000 gi | gigabyte | 950 | 5,91 € | |
| | Monitor | Logging ingestion | gigabyte | 1224 | 5,69 € | |
| | | Logging storage | gigabyte | 979,2 | 0,10 € | |
| | | Cloud Monitoring | (5K metric size, 60 metric x hc | 510 | 0,48 € | |
| | IAM | Active directory | quantity | 2 | 3.086,92 € | |
| | Backup | Storage occupato | GB | 26112 | 0,48 € | Actilio |
| PSN Security & Backup | Professional Services | 10 giorni/mese (Security Posture, Policy Verification) | | | | |
| | Key Vault | Managed HSM and AKV operations (HSN | Secrect manager (100 secret, 100K ops, 1200 mese) | | | |
| | Backup on premise | Storage | | | | |
| | Addictional Security | GPC Access Transparency, GPC Access Approval, Assurant Personnel Controls, Key Access Justifications | | 10 | 4.760,38 € | |
| | | | | **TOTALE Progetto Cloud 2** | **318.610** | |

Per l'elenco completo delle voci di listino si faccia riferimento alla documentazione di gara "Proposta PSN-Listino servizi 2.0", Guida Secure Public Cloud

**PUBLIC CLOUD PSN MANAGED**

| Tipo | Tipologia | Tipo | Unit | Time | Applicazione tradizionale medio piccola | Applicazione tradizionale con molta memoria + NAS | Simulazione applicazione cloud native microservizi | Applicazione cloud native microservizi in PaaS | Applicazione analisi fatture basata su Document AI | Applicazione di prenotazioni appuntamenti (i.e. CUP) basata su Conversazionale AI | Serverless Analytics a Consumo con Dashboard di visualizzazione | Applicazione Serverless Analytics Flat con Dashboard di visualizzazione | Applicazione PaaS per gestire appuntamenti via web | Soluzione DevOps CI/CD | Applicazione con molta memoria ed Exadata | Prezzo servizio esposto dal PSN annuo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Licensed Cloud Hyperscaler Technology | vCPUs (vCPU/hour). Committement 3 anni | General Purpose N2 | vCPU | Hour | | 24 | 24 | | | | | | | 2 | 96 | 118,98 € |
| | | Compute optimized | vCPU | hour | 8 | | | | | | | | | | | 113,69 € |
| | | Memory-optimized | vCPU | hour | | | | | | | | | | | | 87,36 € |
| | | Shared Core (Burstable e2-Micro Instance) | vCPU | hour | | | | | | | | | | | | 31,55 € |
| | | Accellerated Core A2 | vCPU | hour | | | | | | | | | | | | 92,54 € |
| | VMs Single Tenant | Sole Tenancy Compute Optimized Core | vCPU | hour | | | | | | | | | | | | 284,22 € |
| | | Sole Tenancy Compute Optimized RAM | gigabyte | hour | | | | | | | | | | | | 35,48 € |
| | | Sole Tenancy Memory Optimized Core | vCPU | hour | | | | | | | | | | | | 82,09 € |
| | | Sole Tenancy Memory Optimized RAM | gigabyte | hour | | | | | | | | | | | | 271,30 € |
| | Memory (GB/hour). Committment 3 anni | Accelerated Instances RAM | gigabyte | hour | | | | | | | | | | | | 86,18 € |
| | | General Purpose RAM | gigabyte | hour | 16 | 192 | 64 | | | | | | | 2 | 384 | 12,92 € |
| | | Memory Instances RAM | gigabyte | hour | | | | | | | | | | | | 11,97 € |
| | | Compute Optimezed RAM | gigabyte | hour | | | | | | | | | | | | 35,48 € |
| | | Shared RAM (Burstable e2-Micro Instance) | gigabyte | hour | | | | | | | | | | | | 26,70 € |
| | | Extended Memory (Custom Extended Instance Ram) | gigabyte | hour | 24 | 48 | | | | | | | | | | 74,40 € |
| | Confidential Computing | Confidential Computing Instance Core | vCPU | hour | | | | | | | | | | | | 41,66 € |
| | | Confidential Computing Instance RAM | gigabyte | hour | | | | | | | | | | | | 5,20 € |
| Licensed Cloud Persistent Storage Hyperscaler Technology | Storage | Persistent Disk Standard | gigabyte | hour | 200 | | | | | | | | | | | 0,78 € |
| | | Persistent Disk SSD | gigabyte | hour | | 1000 | 400 | | | | | | | | 1200 | 1,65 € |
| | | Balanced PD | gigabyte | hour | | | | | | | | | | 2 | | 0,97 € |
| | | Extreme PD IOPS | gigabyte | hour | | | | | | | | | | | | 1,21 € |
| | | PD Snapshot | gigabyte | hour | | | | | | | | | | | | 184,11 € |
| | | Opzione Protezione Multi Region | gigabyte | hour | | | | | | | | | | | | 202,52 € |
| | | NFS storage | gigabyte | hour | | 1000 | | | | | | | | | | 6,40 € |
| | | Filestore Backup Storage | gigabyte | hour | | | | | | | | | | | | 0,87 € |
| Licensed Cloud Storage Hyperscaler Technology | Cloud Storage | Archive Storage Multi-region | gigabyte | hour | | | | | | | | | | | | 0,04 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 217,46 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 3.801,70 € |
| | | Data Retrivial Operations | gigabyte | | | | | | | | | | | | | 354,06 € |
| | | Coldline Storage Multi-region | gigabyte | hour | | | | | | | | | | | | 0,07 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 76,03 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 380,17 € |
| | | Data Retrivial Operations | gigabyte | | | | | | | | | | | | | 141,62 € |
| | | Durable Reduced Availability Storage | gigabyte | hour | | | | | | | | | | | | 0,19 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 76,03 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 76,03 € |
| | | Standard Storage Multi-region | gigabyte | hour | | | | | | | | | | | | 0,25 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 38,02 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 30,41 € |
| | | Nearline Storage Multi-region | gigabyte | hour | | | | | | | | | | | | 0,10 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 760,34 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 760,34 € |
| | | Data Retrivial Operations | gigabyte | | | | | | | | | | | | | 70,81 € |
| | | Standard Storage Regional | gigabyte | hour | | | | | | | | | | | | 0,19 € |
| | | Class A Operations | 1000 | count | | | | | | | | | | | | 380,17 € |
| | | Class B Operations | 10000 | count | | | | | | | | | | | | 304,14 € |
| Networking | VPN | VPN TUNNEL | tunnel | hour | | | | | | | | | | | | 380,17 € |
| | | VPN Traffic Egress EMEA 0 to 1,024 gibibyte | gigabyte | hour | | | | | | | | | | | | 1,16 € |
| | | VPN Traffic Egress EMEA 1,024 to 10,240 | gigabyte | hour | | | | | | | | | | | | 1,07 € |
| | | VPN Traffic Egress EMEA 10,240 gibibyte and above, | gigabyte | hour | | | | | | | | | | | | 0,78 € |
| | Static IP | Static IP charge (VM external or VPN Gateway) | per ip | hour | 1 | | | | | | | | | | | 76,03 € |
| | Partner Interconnect | Cloud Interconnect for MPS - 10Gbps Partner circuit | circuit | hour | | | | | | | | | | | | 17.944,02 € |
| | | Cloud Interconnect for MPS - 100Gbps Partner circuit | circuit | hour | | | | | | | | | | | | 137.241,31 € |
| | | Cloud Interconnect - 100Mbps VLAN attachment via Google partner | vlan attachment | hour | | | | | | | | | | | | 475,21 € |
| | | Cloud Interconnect - 1Gbps VLAN attachment via Google partner | vlan attachment | hour | | | | | | | | | | | | 2.112,22 € |
| | | Cloud Interconnect - 10Gbps VLAN attachment via Google partner | vlan attachment | hour | | | | | | | | | | | | 17.944,02 € |
| | | America/Europe) | gigabyte | | | | | | | | | | | | | 141,62 € |
| | NAT Gateway | NAT Gateway: Data processing charge in Belgium | gigabyte | | | | | | | | | | | | | 318,66 € |
| | | NAT Gateway: Uptime charge in Belgium | instance | hour | | | | | | | | | | | | 10,64 € |
| | External Cloud Load Balancer | Networking Cloud Load Balancing HTTPS External Regional Forwarding Rule I | project) | hour | 1 | 10 | 10 | 10 | | | | | | | 10 | 83,64 € |
| | | Networking Cloud Load Balancing HTTPS External Regional Inbound Data Pro | gigabyte | | | 1 | 1 | 1 | | | | | | | 1 | 57,36 € |
| | Internal Network Load Balancer or HTTPS Load balancer | Forwarding Rule Minimum Service Charge in EMEA | rule | hour | | | | | | | | | | | | 190,08 € |
| | | Forwarding Rule Additional Service Charge in EMEA | rule | hour | | | | | | | | | | | | 76,03 € |
| | | Data Processing Charge in EMEA | gigabyte | | | | | | | | | | | | | 56,65 € |
| | Cloud DNS | DNS Query (port 53) 0 to 1,000,000,000 count | per 1,000,000 count | hour | | | | | | | | | | | | 4,17 € |
| | | DNS Query (port 53) 1,000,000,000 count and above | per 1,000,000 count | hour | | | | | | | | | | | | 2,08 € |
| | | ManagedZone for 0 to 25 | per zone | hour | | | | | | | | | | | | 2,08 € |
| | | ManagedZone 25 to 10,000 | per zone | hour | | | | | | | | | | | | 2,08 € |
| | | ManagedZone 10,000 month and above | per zone | hour | | | | | | | | | | | | 2,26 € |
| | CDN | Cache Egress to Europe | gigabyte | hour | | | | | | | | | | | | 0,24 € |

**PUBLIC CLOUD PSN MANAGED**

| Tipo | Tipologia | Tipo | Unit | Time | Applicazione tradizionale medio piccola | Applicazione tradizionale con molta memoria + NAS | Simulazione applicazione cloud native microservizi | Applicazione cloud native microservizi in PaaS | Applicazione analisi fatture basata su Document AI | Applicazione di prenotazioni appuntamenti (i.e. CUP) basata su Conversazionale AI | Serverless Analytics a Consumo con Dashboard di visualizzazione | Applicazione Serverless Analytics Flat con Dashboard di visualizzazione | Applicazione PaaS per gestire appuntamenti via web | Soluzione DevOps CI/CD | Applicazione con molta memoria ed Exadata | Prezzo servizio esposto dal PSN annuo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | CDN | Cache Lookup Requests | 10000 | count | | | | | | | | | | | | 57,03 € |
| | Egress to Internet | Egress to EMEA | gigabyte | hour | 0,1 | | | | | | | | | | | 1,84 € |
| Licensed Kubernetes Hyperscaler Technology | Kubernetes | Kubernetes Engine Autopilot | cluster | hour | | | | | | | | | | | | 41,82 € |
| | | Autopilot Pod mCPU | vCPU | hour | | | | 12 | | | | | | | | 372,57 € |
| | | Autopilot Pod Ephemeral Storage | gigabyte | hour | | | | 48 | | | | | | | | 0,43 € |
| | | Autopilot Pod Memory | gigabyte | hour | | | | 24 | | | | | | | | 38,38 € |
| | | Regional Kubernetes Clusters | cluster | hour | | | | | | | | | | | | 760,34 € |
| | | Zonal Kubernetes Clusters | cluster | hour | | | | | | | | | | | | 760,34 € |
| | | Multi-cluster Ingress backend Pod-hours (standalone) | pod | hour | | | | | | | | | | | | 31,25 € |
| | | Cloud Build | Build time | hour | | | | | | | | | | 3 | | 1.368,61 € |
| | | Cloud Source Repository | Active users | hour | | | | | | | | | | 10 | | 10,42 € |
| | | Cloud Run (tier 1) | | | | | | | | | | | | | | - € |
| | | CPU | vCPU | hour | | | | | | | | | 1 | | | 656,93 € |
| | | Memory | gigabyte | hour | | | | | | | | | 128 | | | 63,73 € |
| | | Requests | 1M requests | hour | | | | | | | | | 10 | | | 4,17 € |
| Licensed SQL e Oracle Hyperscaler Technology | SQL instances | PostgresSQL no HA , MySQL no HA | | | | | | | | | | | | | | - € |
| | | vCPU | vCPU | hour | | | | | | | | | | | | 150,70 € |
| | | RAM | gigabyte | hour | | | | | | | | | | | | 23,79 € |
| | | Storage Capacity (SSD) | gigabyte | hour | | | | | | | | | | | | 1,65 € |
| | | Storage Capacity (HDD) | gigabyte | hour | | | | | | | | | | | | 0,87 € |
| | | Storage (Backup) - used | gigabyte | hour | | | | | | | | | | | | 0,78 € |
| | | PostgresSQL Regional (HA), MySQL Regional (HA) | | | | | | | | | | | | | | - € |
| | | vCPU | vCPU | hour | | 8 | 8 | 8 | | | | | | | | 301,47 € |
| | | RAM | gigabyte | hour | | 52 | 64 | 64 | | | | | | | | 47,59 € |
| | | Storage Capacity (SSD) | gigabyte | hour | | 1024 | 256 | 256 | | | | | | | | 3,30 € |
| | | Storage Capacity (HDD) | gigabyte | hour | | | | | | | | | | | | 1,75 € |
| | | Storage (Backup) - used | gigabyte | hour | | 2048 | | | | | | | | | | 0,78 € |
| | | SQLServer no HA | | | | | | | | | | | | | | - € |
| | | vCPU | vCPU | hour | 8 | | | | | | | | | | | 150,70 € |
| | | RAM | gigabyte | hour | 16 | | | | | | | | | | | 23,79 € |
| | | Storage Capacity (SSD) | gigabyte | hour | 512 | | | | | | | | | | | 1,65 € |
| | | Storage (Backup) - used | gigabyte | hour | 1024 | | | | | | | | | | | 0,78 € |
| | | | | | | | | | | | | | | | | - € |
| | | SQLServer Regional (HA) | | | | | | | | | | | | | | - € |
| | | vCPU | vCPU | hour | | | | | | | | | | | | 301,47 € |
| | | RAM | gigabyte | hour | | | | | | | | | | | | 47,59 € |
| | | Storage Capacity (SSD) | gigabyte | hour | | | | | | | | | | | | 3,30 € |
| | | Storage (Backup) - used | gigabyte | hour | | | | | | | | | | | | 0,78 € |
| | | BigQuery | | | | | | | | | | | | | | - € |
| | | Queries (on-demand) | gigabyte | hour | | | | | | | 5000000 | | | | | 0,00 € |
| | | Flat Annual (min 100 slot) | slot | hour | | | | | | | | 1000 | | | | 17,71 € |
| | | Storage Active | gigabyte | hour | | | | | | | 10240 | 10240 | | | | 0,19 € |
| | | Storage Long-Term | gigabyte | hour | | | | | | | | | | | | 0,10 € |
| | | Data Studio | | | | | | | | | 100 | 100 | | | | - € |
| | | Oracle Database Exadata Cloud at Customer - Database OCPU | OCPU | hour | | | | | | | | | | | | 10.161,40 € |
| | | Oracle Database Exadata Cloud at Customer - Database OCPU - BYOL | OCPU | hour | | | | | | | | | | | 8 | 2.438,83 € |
| | | Gen 2 Exadata Cloud at Customer - Database OCPU | OCPU | hour | | | | | | | | | | | | 10.161,40 € |
| | | Gen 2 Exadata Cloud at Customer - Database OCPU - BYOL | OCPU | hour | | | | | | | | | | | | 2.438,83 € |
| | | Exadata Cloud at Customer - Autonomous Transaction Processing - Database | OCPU | hour | | | | | | | | | | | | 10.161,40 € |
| | | Exadata Cloud at Customer - Autonomous Data Warehouse - Database OCPU | OCPU | hour | | | | | | | | | | | | 10.161,40 € |
| | | Exadata Cloud at Customer - Autonomous Transaction Processing - Database | OCPU | hour | | | | | | | | | | | | 2.438,83 € |
| | | Exadata Cloud at Customer - Autonomous Data Warehouse - Database OCPU | OCPU | hour | | | | | | | | | | | | 2.438,92 € |
| | | NoSQL Document DB ops | 100,000 count | | | | | | | | | | 10 | | | 0,05 € |
| | | NoSQL Document DB storage | gigabyte | hour | | | | | | | | | 50 | | | 1,75 € |
| | | Oracle Autonomous Data Warehouse - Exadata Storage | Terabyte | month | | | | | | | | | | | | 895.101,54 € |
| | | Oracle Autonomous Transaction Processing - Exadata Storage | Terabyte | month | | | | | | | | | | | | 895.101,54 € |
| | | Oracle Database Cloud Service - Standard Edition | OCPU | hour | | | | | | | | | | | | 1.625,41 € |
| | | Oracle Database Cloud Service - Enterprise Edition | OCPU | hour | | | | | | | | | | | | 3.251,54 € |
| | | Oracle Database Cloud Service - Enterprise Edition High Performance | OCPU | hour | | | | | | | | | | | | 6.706,42 € |
| | | Oracle Database Cloud Service - Enterprise Edition Extreme Performance | OCPU | hour | | | | | | | | | | | | 10.161,40 € |
| | | Oracle Database Cloud Service - All Editions - BYOL | OCPU | hour | | | | | | | | | | | | 1.462,82 € |
| | | MySQL Database - Standard - E2' | OCPU | hour | | | | | | | | | | | | 353,01 € |
| | | MySQL Database - Storage | Gbyte | | | | | | | | | | | | | 302,42 € |
| | | MySQL Database - Backup Storage | Storage Capacity Per Month | | | | | | | | | | | | | 302,42 € |
| | | MySQL Database - Bare Metal Standard - E2' | Node | hour | | | | | | | | | | | | 3.793,64 € |
| | | MySQL Database - Standard - E3' | OCPU | hour | | | | | | | | | | | | 287,27 € |
| | | MySQL Database - Standard - E3 - Memory | Gbyte | hour | | | | | | | | | | | | 16,66 € |
| | | Anomaly detection | | | | | | | | | | | | | | - € |
| | | Digital Assistant (CCAI) | | | | | | | | | | | | | | - € |
| | | Standard CCAI Insights natural language analysis | conversation | hour | | | | | | 50000 | | | | | | 0,52 € |

**PUBLIC CLOUD PSN MANAGED**

| Tipo | Tipologia | Tipo | Unit | Time | Applicazione tradizionale medio piccola | Applicazione tradizionale con molta memoria + NAS | Simulazione applicazione cloud native microservizi | Applicazione cloud native microservizi in PaaS | Applicazione analisi fatture basata su Document AI | Applicazione di prenotazioni appuntamenti (i.e. CUP) basata su Conversazionale AI | Serverless Analytics a Consumo con Dashboard di visualizzazione | Applicazione Serverless Analytics Flat con Dashboard di visualizzazione | Applicazione PaaS per gestire appuntamenti via web | Soluzione DevOps CI/CD | Applicazione con molta memoria ed Exadata | Prezzo servizio esposto dal PSN annuo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Licensed AI/ML Hyperscaler Technology | AI ML Platform | Topic Model labeling | conversation | hour | | | | | | 50000 | | | | | | 1,04 € |
| | | Data Science Platform | | | | | | | | | | | | | | - € |
| | | AI HR | | | | | | | | | | | | | | - € |
| | | AI Finance | | | | | | | | | | | | | | - € |
| | | 'general' type pages processed with Form Parser (for 0 to 1M pages) | page | hour | | | | | | | | | | | | 0,68 € |
| | | 'general' type pages processed with Form Parser (above 1M pages) | page | hour | | | | | | | | | | | | 0,52 € |
| | | pages processed for DAI Core Custom Model Prediction | page | hour | | | | | | | | | | | | 0,26 € |
| | | pages processed for OCR processor (FREE for 0 to 1000 pages) | page | hour | | | | | | | | | | | | - € |
| | | pages processed for OCR processor (for 1000 to 5M pages) | page | hour | | | | | | | | | | | | 0,02 € |
| | | pages processed for OCR processor (above 5M pages) | page | hour | | | | | | | | | | | | 0,01 € |
| | | AI Documenti | | | | | | | | | | | | | | - € |
| | | 'general' type pages processed with Form Parser (for 0 to 1M pages) | page | hour | | | | | 100000 | | | | | | | 0,68 € |
| | | 'general' type pages processed with Form Parser (above 1M pages) | page | hour | | | | | | | | | | | | 0,52 € |
| | | pages processed for DAI Core Custom Model Prediction | page | hour | | | | | 100000 | | | | | | | 0,26 € |
| | | pages processed for OCR processor (FREE for 0 to 1000 pages) | page | hour | | | | | | | | | | | | - € |
| | | pages processed for OCR processor (for 1000 to 5M pages) | page | hour | | | | | 50000 | | | | | | | 0,02 € |
| | | pages processed for OCR processor (above 5M pages) | page | hour | | | | | | | | | | | | 0,01 € |
| Licensed Security Cloud Solution | Cloud Security | Security Command Center (brute-force attacks, and SQL injections) | | | | | | | | | | | | | | - € |
| | | Event Threat Detection Log Ingest Bytes | | | | | | | | | | | | | | 1.900,85 € |
| | | Ingress Egress Network Traffic | | | | | | | | | | | | | | 2.281,02 € |
| | | SCC Premium ("Available as either a one year or multi-year fixed price subscription.<br>The annual cost of the subscription is 5% of the larger of:<br>(i) Your committed annual Google Cloud spend; or<br>(ii) Your current Google Cloud spend, annualized<br>The minimum annual cost is 25,000.00 USD.") | | | | | | | | | | | | | | - € |
| | | Access Transparency (Free ingestion but requires certain Google Cloud Support levels) | | | | | | | | | | | | | | - € |
| | | Access Approval (Free but requires certain Google Cloud Support levels) | | | | | | | | | | | | | | - € |
| | | Assurant Personnel Controls (Free but requires certain Google Cloud Support levels) | | | | | | | | | | | | | | - € |
| | | Key Access Justifications | | | | | | | | | | | | | | - € |
| | | | | | | | | | | | | | | | | - € |
| | | Cloud Armor | | | | | 1 | 1 | | | | | | | 1 | 5.765,04 € |
| | | Policies | policy | count | | | | | | | | | | | | 52,08 € |
| | | Rules | rule | count | | | | | | | | | | | | 10,42 € |
| | | Incoming Request | millon requests | count | | | | | | | | | | | | 5.702,55 € |
| | | reCaptcha | | | | | | | | | | | | | | - € |
| | | CreateAssessment Requests (free for for 0 to 1,000,000 requests) | requests | hour | | | | | | | | | | | | - € |
| | | CreateAssessment Requests (for 1,000,000 requests and above) | requests | hour | | | 10000 | 10000 | | | | | | | 10000 | 0,01 € |
| | | reCAPTCHA Enterprise FMF | | hour | | | 1 | 1 | | | | | | | 1 | 10,42 € |
| | | Managed Active Directory | Region | hour | | | | | | | | | | | | 3.041,36 € |
| | Cloud Operations | Cloud Logging | | | | | | | | | | | | | | - € |
| | | Logging ingestion (free from 0 to 50GB) | gigabyte | hour | | | | | | | | | | | | 5,65 € |
| | | Logging storage (logs retained more than 30 days) | gigabyte | hour | | | | | | | | | | | | 0,10 € |
| | | Cloud Monitoring (5K metric size, 60 metric x hours) | metric | hour | | | | | | | | | | | | 0,47 € |
| | | | | | | | | | | | | | | | | - € |
| | Professional Services | 10 giorni/mese (Security Posture, Policy Verification) | | | | | | | | | | | | | | - € |
| | Key Vault | Managed HSM and AKV operations (HSM on premise) | | | | | | | | | | | | | | - € |
| | | | | **TOTALE** | 6.442 | 27.704 | 17.417 | 18.487 | 94.522 | 78.117 | 25.669 | 19.693 | 8.944 | 4.476 | 44.645 | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CLUSTER 1** Tradizionale | **9** | **8** | | | | | | | | | **3** | **413.544 €** |
| **CLUSTER 2** Tradizionale + Microservizi | **7** | **7** | **6** | | | | | | | | | **343.523 €** |
| **CLUSTER 3** Tradizionale + Microservizi e PaaS | **5** | **5** | **5** | **5** | | | | | | | | **350.251 €** |
| **CLUSTER 4** Tradizionale + Microservizi + PaaS e Documentale AI | **3** | **3** | **3** | **3** | **3** | **3** | **2** | | | | | **779.405 €** |
| **CLUSTER 5** Mix tra tradizionale, Microservizi, PaaS, AI e CI/CD | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **1** | **1** | **643.111 €** |

Per l'elenco completo delle voci di listino si faccia riferimento alla documentazione di gara "Proposta PSN-Listino servizi 2.0", Guida Public Cloud PSN Managed

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO D

## SCHEMA CONTRATTO DI UTENZA

# SOMMARIO


**SEZIONE I - DISPOSIZIONI GENERALI** **5**

Articolo 1 PREMESSE E DOCUMENTI CONTRATTUALI 5

Articolo 2 DEFINIZIONI 5

Articolo 3 OGGETTO DEL CONTRATTO 5

Articolo 4 DURATA DEL CONTRATTO 5

**SEZIONE II – ATTIVITÁ PRODROMICHE ALL'AVVIO DELLA GESTIONE DEL SERVIZIO** **6**

Articolo 5 NOMINA DEI REFERENTI DELLE PARTI 6

Articolo 6 PREDISPOSIZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO 6

Articolo 7 ACCETTAZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO 6

**SEZIONE III – FASE DI GESTIONE DEL SERVIZIO** **7**

Articolo 8 AVVIO DELLA FASE DI GESTIONE DEL SERVIZIO 7

Articolo 9 MODALITÁ DI PRESTAZIONE DEL SERVIZIO 7

Articolo 10 CORRISPETTIVO PER IL SERVIZIO 7

Articolo 11 PERIODICITÀ DEI PAGAMENTI E FATTURAZIONE 8

Articolo 12 MODIFICHE IN CORSO DI ESECUZIONE 8

Articolo 13 VERIFICHE IN CORSO DI ESECUZIONE 9

Articolo 14 PROCEDURA DI CONTESTAZIONE DEI DISSERVIZI E PENALI 9

**SEZIONE IV – GARANZIE E POLIZZE ASSICURATIVE** **10**

Articolo 15 GARANZIE 10

Articolo 16 POLIZZE ASSICURATIVE 11

Articolo 17 GARANZIE DEL CONCESSIONARIO PER I FINANZIATORI 11

**SEZIONE V – VICENDE DEL CONTRATTO** **11**

Articolo 20 REVOCA E RISOLUZIONE PER INADEMPIMENTO DELL'AMMINISTRAZIONE UTENTE 12

Articolo 21 RECESSO 13

Articolo 22 SCADENZA DEL CONTRATTO 13

**SEZIONE VI – ULTERIORI DISPOSIZIONI** **14**

Articolo 23 COMUNICAZIONI 14

Articolo 24 NORME ANTICORRUZIONE E ANTIMAFIA, PROTOCOLLI DI LEGALITÀ 14

Articolo 25 OBBLIGHI IN TEMA DI TRACCIABILITÀ DEI FLUSSI FINANZIARI 14

Articolo 26 CONTROVERSIE E FORO COMPETENTE 15

Articolo 27 TRATTAMENTO DEI DATI PERSONALI 15

Articolo 28 REGISTRAZIONE 15

Articolo 29 RINVIO AL CODICE CIVILE E AD ALTRE DISPOSIZIONI DI LEGGE VIGENTI 15

# CONTRATTO DI UTENZA

L'anno [•], il giorno [•] del mese di [•],

tra

[•] con sede in [•], [•] n. [•] codice fiscale [•], nella persona del [•] [•], in qualità di [•], nato a [•], il [•], C.F.

[•] ("[•]" o "**Amministrazione Utente**")

**e**

**La Società Polo Strategico Nazionale S.p.A** ("**PSN S.p.A**.") con sede legale in Roma, via Goito 4, numero di iscrizione nel Registro delle Imprese di Roma 1678264, Codice Fiscale e Partita IVA 16825251008 in persona del dott. Massimo Mancini, nato a Campobasso (CB) il 12/07/1963, C.F. MNCMSM63L12B519G e domiciliato ai fini del presente contratto in via Goito 4, nella qualità di Presidente del Consiglio di Amministrazione e rappresentante legale

in seguito denominati, rispettivamente, "**Parte**" al singolare, o, congiuntamente, "**Parti**".

## PREMESSO CHE

1. Le società TIM S.p.A., CDP Equity S.p.A., Leonardo S.p.A. e Sogei S.p.A. ("**Proponente**") hanno presentato, in forma di costituendo raggruppamento temporaneo di imprese, ai sensi degli artt. 164, 165, 179, comma 3 e 183, comma 15 del d. lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni ("**Codice**"), una proposta avente ad oggetto l'affidamento di una concessione relativa, in particolare, alla prestazione da parte del Concessionario in favore delle singole Amministrazioni Utenti, in maniera continuativa e sistematica, di un Catalogo di Servizi, con messa a disposizione di un'infrastruttura digitale per i servizi infrastrutturali e applicativi in *cloud* per la gestione di dati sensibili - "Polo Strategico Nazionale" - appositamente progettata, predisposta ed allestita, con caratteristiche adeguate ad ospitare la migrazione dei dati frutto della razionalizzazione e consolidamento dei Centri di elaborazione Dati e relativi sistemi informatici delle pubbliche amministrazioni di cui all'articolo 33 *septies* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'articolo 35 del d.l. 16 luglio 2020, n. 76 nonché come ulteriormente modificato dall'art. 7 del D.L. 6 novembre 2021, n. 152 ed a ricevere la migrazione dei detti dati perché essi siano poi gestiti attraverso una serie di servizi da rendere alle amministrazioni titolari dei dati stessi, vale a dire Servizi Infrastrutturali; Servizi di Gestione della Sicurezza IT; Servizi di *Disaster recovery* e *Business Continuity*; Servizi di Assistenza ("**Proposta**").

2. La Proposta è stata elaborata con il proposito di inserirsi nell'ambito degli obiettivi indicati dal Piano Nazionale di Ripresa e Resilienza, con particolare riferimento agli "Obiettivi Italia Digitale 2026", e dal decreto-legge 16 luglio 2020, n. 76, per come convertito dalla legge 21 maggio 2021, n. 69, nonché di quelli dettati dall'Agenzia per l'Italia Digitale per la realizzazione dell'Agenda Digitale Italiana, in coerenza con gli indirizzi del Presidente del Consiglio dei Ministri e del Ministro delegato, e in particolare dell' "Obiettivo 3 – Cloud e Infrastrutture Digitali" orientato alla migrazione dei dati e degli applicativi informatici delle pubbliche amministrazioni. In questo

contesto, e con particolare riferimento alla razionalizzazione e al consolidamento dei Data Center della Pubblica Amministrazione, si inserisce l'identificazione e la creazione del "Polo Strategico Nazionale" (nel séguito anche solo "**PSN**"). Conseguentemente, la Proposta veniva espressamente inquadrata dal Proponente nell'ambito del perseguimento degli obiettivi del Piano Nazionale di Ripresa e Resilienza e, in particolare, dell'obiettivo di «Digitalizzare la Pubblica Amministrazione italiana con interventi tecnologici ad ampio spettro accompagnati da riforme strutturali» di cui alla Missione 1, Componente M1C1.

3. Il DTD valutava la Proposta presentata dalla TIM S.p.A., in qualità di mandataria del costituendo RTI con CDP Equity S.p.A., Leonardo S.p.A. e Sogei S.p.A., formulando alcune osservazioni, e - al fine di fornire la massima efficacia alla tutela dell'interesse pubblico perseguito - invitava il Proponente, con richiesta a mezzo PEC del 2 dicembre 2021 (protocollo DTD-3651-P e DTD-3652-P), ai sensi di quanto previsto dall'articolo 183, comma 15, del Codice, ad apportare specifiche modifiche al progetto di fattibilità; essendosi il Proponente uniformato alle osservazioni ricevute nel termine indicato, la Proposta veniva ulteriormente valutata.

4. Ad esito delle suddette valutazioni, il DTD si esprimeva favorevolmente circa la fattibilità della Proposta, in quanto rispondente alla necessità dello stesso DTD di avvalersi di soggetti privati per soddisfare le esigenze delle Amministrazioni e per il conseguimento degli obiettivi di pubblico interesse individuati dal Piano Nazionale di Ripresa e Resilienza, dal d.l. 16 luglio 2020, n. 76 e dall'Agenzia per l'Italia Digitale per la realizzazione dell'Agenda Digitale Italiana;

5. Il DTD, con provvedimento adottato dal Capo del Dipartimento per la trasformazione digitale n. 47/2021-PNRR del 27/12/2021, dichiarava quindi la Proposta fattibile, ponendola in approvazione e nominando, contestualmente, il Proponente come promotore ("**Promotore**").

6. Difesa Servizi S.p.A., in qualità di Centrale di Committenza - in virtù della convenzione sottoscritta il 25 dicembre 2021 con il Dipartimento per la trasformazione digitale e il Ministero della Difesa - indiceva, con determina a contrarre n. 3 del 28/01/2022, ai sensi degli artt. 3, comma 1, lett. eee), 60 e 180 nonché 183, commi 15 e 16 del Codice, la Gara europea, a procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico – privato, della realizzazione e gestione del Polo Strategico Nazionale, CIG: 9066973ECE CUP: J51B21005710007, con bando, inviato per la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea in data 28/01/2022 e pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 15 del 04/02/2022.

7. La Commissione giudicatrice, nominata con provvedimento n. 3 del 14/04/2022, con verbali n. 5 del 10/06/2022, n. 6 del 14/06/2022 e n. 7 del 15/06/2022, formulava la proposta di aggiudicazione a favore del costituendo RTI tra Aruba S.p.A. e Fastweb S.p.A. in qualità di mandataria ("**RTI Fastweb**"). La graduatoria di Gara veniva approvata con determina n. 14 del 22/06/2022 della Centrale di Committenza e comunicata agli operatori economici partecipanti alla Gara con comunicazioni rispettivamente n. 2402 e n. 2403 di protocollo del 22/06/2022. Il Promotore, non risultato aggiudicatario, esercitava, nel termine previsto dall'art. 183, comma 15 del Codice, con comunicazione del giorno 07/07/2022, protocollo in entrata della Centrale di Committenza n. 2362, il diritto di prelazione di cui all'art. 183, comma 15, del Codice, impegnandosi ad adempiere a tutte le obbligazioni contrattuali alle medesime condizioni offerte dall'operatore economico individuato come aggiudicatario originario della procedura di Gara. Il Promotore, con determina di aggiudicazione della Centrale di Committenza n. 15 del 11/07/2022, comunicata agli operatori economici partecipanti alla Gara con comunicazione rispettivamente n. 2681 e n. 2682 di protocollo del 11/07/2022, veniva per l'effetto dichiarato nuovo aggiudicatario della procedura.

8. Successivamente all'esercizio del diritto di prelazione, in data 04/08/2022, i componenti del RTI Proponente, ai sensi dell'art. 184 del Codice, hanno costituito la Società di Progetto denominata Polo Strategico Nazionale S.p.A.

9. Il giorno 24/08/2022 veniva stipulata la relativa convenzione di concessione ("**Convenzione**") tra il DTD e la Società di Progetto Polo Strategico Nazionale S.p.A.

10. Il giorno [•][•][•], l'Amministrazione Utente presentava al Concessionario il proprio Piano dei Fabbisogni, così come definito all'art. 2, lett. zzyy. della Convenzione, contenente, per ciascuna categoria di Servizi, indicazioni di tipo quantitativo con riferimento a ciascun servizio che la stessa intende acquistare in cambio del pagamento di un prezzo.

11. Il giorno [•][•][•], il Concessionario ha presentato all'Amministrazione Utente il Progetto del Piano dei Fabbisogni, così come definito all'art. 2, lett. eee. della Convenzione, nel quale sono raccolte e dettagliate le richieste dell'Amministrazione Utente, contenute nel Piano dei Fabbisogni, e la relativa proposta tecnico/economica secondo le modalità tecniche ed i listini previsti rispettivamente nel Capitolato Servizi e nel Catalogo Servizi.

12. Il giorno [•][•][•], il Concessionario ha presentato all'Amministrazione Utente il Piano Migrazione di Massima, così come definito all'art. 2, lett. aaa. della Convenzione, contenente l'ipotesi di migrazione del Data Center dell'Amministrazione Utente nel Polo Strategico Nazionale.

13. In applicazione di quanto stabilito all'art. 5 della Convenzione, l'Amministrazione Utente intende aderire alla Migrazione, come definita all'art. 2, lett. qq. della Convenzione stessa, per la realizzazione del Piano dei Fabbisogni presentato al Concessionario, attraverso la stipula di apposito Contratto, come definito alla lett. q. del medesimo articolo.

14. L'Amministrazione Utente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto.

15. L'Amministrazione Utente - in ottemperanza alla vigente normativa in materia di sicurezza sui luoghi di lavoro - ha integrato il "Documento di valutazione dei rischi standard da interferenze" allegato ai documenti di gara, riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato il presente Contratto, indicando i costi relativi alla sicurezza.

16. il CIG del presente Contratto è il seguente: [•].

17. il Codice univoco ufficio per Fatturazione è il seguente: [•].

Tutto ciò premesso, le Parti convengono e stipulano quanto segue:

## SEZIONE I - DISPOSIZIONI GENERALI

### Articolo 1
### PREMESSE E DOCUMENTI CONTRATTUALI

1. Le premesse e gli allegati, ancorché non materialmente allegati al Contratto, ne costituiscono parte integrante e sostanziale.

2. Costituiscono, altresì, parte integrante e sostanziale del Contratto:

   a) la Convenzione e i relativi allegati;

   b) il Progetto del Piano dei Fabbisogni, redatto dal Concessionario e accettato dall'Amministrazione Utente ai sensi dei successivi artt. 6 e 7, allegato al presente Contratto.

3. Per tutto quanto non espressamente regolato dal Contratto, trovano applicazione la Convenzione, inclusi i relativi allegati, oltre alle norme generali di riferimento di cui all'art. 29.

**Articolo 2**
**DEFINIZIONI**

1. I termini contenuti nel Contratto, declinati sia al singolare, sia al plurale, hanno il significato specificato nella Convenzione e nei relativi allegati.

**Articolo 3**
**OGGETTO DEL CONTRATTO**

1. Il Contratto regola le specifiche condizioni di fornitura all'Amministrazione Utente dei Servizi indicati dal Progetto del Piano dei Fabbisogni, redatto dal Concessionario e accettato dall'Amministrazione Utente ai sensi dei successivi artt. 6 e 7.

**Articolo 4**
**DURATA DEL CONTRATTO**

1. Il Contratto ha la durata complessiva di anni 10 (dieci), a decorrere dalla data di avvio della gestione del Servizio, come individuata dal successivo art. 8.

2. Le Parti espressamente concordano che, in caso di proroga della Convenzione, il Contratto si intenderà prorogato di diritto per una durata corrispondente a quella della proroga della Convenzione.

3. Resta inteso che, in nessun caso, la durata del Contratto potrà eccedere la durata della Convenzione.

## SEZIONE II – ATTIVITÁ PRODROMICHE ALL'AVVIO DELLA GESTIONE DEL SERVIZIO

**Articolo 5**
**NOMINA DEI REFERENTI DELLE PARTI**

1. Entro 10 (dieci) giorni dalla stipula del Contratto:

   a) il Concessionario si impegna a nominare un Direttore del Servizio e un Referente del Servizio, così come definiti all'art. 2, lett. x. e kkk. della Convenzione;

   b) l'Amministrazione Utente si impegna a nominare un Direttore dell'Esecuzione, così come definito all'art. 2, lett. w. della Convenzione.

**Articolo 6**
**PREDISPOSIZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO**

1. Entro 60 (sessanta) giorni dalla stipula del Contratto, il Concessionario dovrà trasmettere all'Amministrazione Utente il Piano di Migrazione di Dettaglio, come definito all'art. 2, lett. bbb. della Convenzione, redatto sulla base del Progetto del Piano dei Fabbisogni e del Piano di Migrazione di Massima presentato all'Amministrazione Utente e contenente le attività e il piano temporale di dettaglio relativi alla migrazione del Data Center dell'Amministrazione Utente nel PSN.

2. Resta inteso che l'Amministrazione Utente si impegna, per quanto di propria competenza, a collaborare con il Concessionario alla redazione del progetto di dettaglio di cui al comma precedente, nonché degli eventuali allegati, e a fornire tempestivamente il supporto che si rendesse necessario, nell'ottica di garantire in buona fede il tempestivo avvio della gestione del Servizio.

## Articolo 7
## ACCETTAZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO

1. L'Amministrazione Utente è tenuta a comunicare al Concessionario l'accettazione Piano di Migrazione di Dettaglio, entro 10 (dieci) giorni dalla presentazione dello stesso.

2. È fatta salva la possibilità per l'Amministrazione Utente di presentare osservazioni al Piano di Migrazione di Dettaglio, nel termine di 10 (dieci) giorni dalla ricezione, con solo riferimento alle modalità di esecuzione delle attività di Migrazione e alla relativa tempistica, dettate da specifiche oggettive esigenze dell'Amministrazione Utente stessa.

3. Le osservazioni dell'Amministrazione Utente saranno discusse in buona fede con il Direttore del Servizio e gli eventuali ulteriori rappresentanti del Concessionario, sia laddove evidenzino criticità, perché si individuino in modo collaborativo le misure adatte al loro superamento, sia perché possano formare oggetto di conoscenza e miglioramento del progetto di dettaglio, laddove mettano in luce elementi positivi suscettibili di ulteriore implementazione o estensione.

4. Tenuto conto delle risultanze del dialogo di cui al comma 3 del presente articolo, il Concessionario provvederà alle conseguenti modifiche al Piano di Migrazione di Dettaglio, nei 10 (dieci) giorni successivi alla ricezione delle osservazioni.

5. Nel caso in cui l'Amministrazione Utente non provveda all'accettazione del Piano di Migrazione di Dettaglio, così come emendato ai sensi del comma precedente, entro i successivi 10 (dieci) giorni, della questione sarà investito il Comitato di controllo costituito ai sensi della Convenzione.

# SEZIONE III – FASE DI GESTIONE DEL SERVIZIO

## Articolo 8
## AVVIO DELLA FASE DI GESTIONE DEL SERVIZIO

1. Il Concessionario è tenuto a dare avvio alla fase di gestione del Servizio nel rispetto dei termini previsti dal Piano di Migrazione di Dettaglio di cui all'art. 6, accettato dall'Amministrazione Utente ai sensi del precedente art. 7.

2. Resta inteso che l'Amministrazione Utente presterà la propria piena collaborazione per l'ottimizzazione della Migrazione, se del caso obbligandosi a far sì che tale collaborazione sia prestata in favore del Concessionario da parte di ogni altro soggetto preposto alla gestione dei centri per l'elaborazione delle informazioni (CED) e dei relativi sistemi informatici dell'Amministrazione Utente stessa, anche laddove gestiti da società in *house*.

3. Resta, altresì inteso che al Concessionario non potranno essere addebitate penali per eventuali ritardi nell'avvio della gestione, qualora tali ritardi siano imputabili all'Amministrazione Utente, anche per il caso di inadempimento a quanto previsto dal comma precedente.

## Articolo 9
## MODALITÁ DI PRESTAZIONE DEL SERVIZIO

1. I Servizi oggetto del Contratto, per come individuati dal progetto di dettaglio di cui all'art. 6, dovranno essere prestati nel rispetto di quanto previsto dal Contratto stesso, nonché della Convenzione e del Capitolato Servizi, al fine di garantire il rispetto dei Livelli di Servizio ("LS" o "SLA"), descritti nell'Allegato H "Indicatori di Qualità".

2. La specificazione degli inadempimenti che comportano, relativamente alle attività oggetto della Convenzione, l'applicazione delle penali, nonché l'entità delle stesse, sono disciplinati nell'Allegato H – "Indicatori di Qualità".

## Articolo 10
## CORRISPETTIVO PER IL SERVIZIO

1. Il Concessionario applicherà i prezzi contenuti nel Catalogo dei Servizi e le condizioni di cui al Capitolato Servizi per ciascuno dei Servizi oggetto del presente Contratto, la cui somma complessiva, prevista nel Progetto del Piano dei Fabbisogni, costituisce il Corrispettivo massimo del Servizio, fatte salve le variazioni che derivino dalle modifiche di cui al successivo art. 13 e quanto previsto all'art. 5 comma 4 lettera ii, all'art. 5 comma 6 e all'art. 11 della Convenzione

2. Si chiarisce che ogni corrispettivo o importo definito nel presente Contratto o nei suoi allegati deve intendersi oltre IVA, se dovuta.

## Articolo 11
## PERIODICITÀ DEI PAGAMENTI E FATTURAZIONE

1. Fermo restando quanto previsto dall'art. 24 della Convenzione, il Corrispettivo del Servizio, determinato ai sensi del precedente art. 10, è versato dall'Amministrazione Utente al Concessionario, con cadenza bimestrale posticipata, a partire dalla data di avvio della fase di gestione, per come individuata ai sensi del precedente art. 8, e a fronte dell'effettiva fornitura del Servizio nel bimestre di riferimento, secondo quanto previsto dal presente Contratto, secondo quanto disposto dal precedente art. 9.

2. Entro 10 (dieci) giorni dal termine del bimestre di riferimento, la fattura relativa ai corrispettivi maturati viene emessa ed inviata dal Concessionario all'Amministrazione Utente, la quale procederà al relativo pagamento entro 30 (trenta) giorni dalla ricezione.

3. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti percentuali, secondo quanto previsto dall'art. 5 del d. lgs. n. 231/2002.

4. L'Amministrazione Utente potrà operare sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5% (zerovirgolacinque per cento) che verrà liquidata dalla stessa solo al termine del presente Contratto e previa acquisizione del documento unico di regolarità contributiva.

5. Fermo restando quanto previsto dall'art. 30, commi 5, 5-*bis* e 6 del Codice e dall'art. 24 della Convenzione, in relazione al caso di inadempienze contributive o retributive, e relative trattenute, i pagamenti avvengono dietro presentazione di fattura fiscale, con modalità elettronica, nel pieno rispetto degli obblighi di tracciabilità dei flussi finanziari, di cui all'art. 3, legge 13 agosto 2010, n. 136 e successive modificazioni o integrazioni, mediante bonifico bancario sul conto [•] o, fermo il rispetto delle norme sulla tracciabilità dei flussi finanziari, su altro conto corrente intestato al Concessionario ed indicato nel Contratto, e previa indicazione di CIG nella causale di pagamento. A tal fine, il Concessionario indica nel Contratto i seguenti soggetti abilitati a operare sul suddetto conto: [•].

## Articolo 12
## MODIFICHE IN CORSO DI ESECUZIONE

1. L'Amministrazione Utente ha la facoltà di richiedere per iscritto modifiche in corso di esecuzione per far fronte ad eventuali nuove e diverse esigenze emerse in fase di attuazione.

2. Qualora le modifiche proposte riguardino il Piano di Migrazione di Dettaglio, nel termine di 30 (trenta) giorni dalla ricezione delle richieste di modifica, il Concessionario presenterà all'Amministrazione Utente un nuovo Piano di Migrazione di Dettaglio. L'Amministrazione Utente provvederà all'accettazione secondo la procedura delineata dall'art. 7 del presente Contratto. Tali variazioni sono adottate in tempo utile per consentire al Concessionario di garantire l'erogazione dei servizi.

3. Qualora le modifiche proposte riguardino il Progetto del Piano dei Fabbisogni trovano applicazione, in quanto compatibili, gli art. 106, comma 2 e 175, comma 4 del Codice.

4. Nel caso in cui le modifiche proposte ai sensi del comma precedente non superino la soglia di cui al 10% (dieci per cento) del valore iniziale del Contratto, l'Amministrazione Utente procederà con la presentazione al Concessionario di nuovo Piano dei Fabbisogni, sulla base del quale il Concessionario redigerà un nuovo Progetto del Piano dei Fabbisogni, che sarà poi accettato dall'Amministrazione Utente secondo la procedura delineata all'art. 18 della Convenzione. Il Progetto del Piano dei Fabbisogni accettato dall'Amministrazione Utente a norma del presente comma sostituirà il progetto originario allegato al presente Contratto. La predisposizione del Piano di Migrazione di Dettaglio conseguente segue la procedura delineata all'art. 7 del presente Contratto.

## Articolo 13
## VERIFICHE IN CORSO DI ESECUZIONE

1. Fermo quanto previsto dalla Convenzione, l'Amministrazione Utente avrà facoltà di eseguire verifiche relative al rispetto di quanto previsto dal Contratto stesso, della Convenzione e dei Livelli di Servizio ("LS" o "SLA"), descritti nell'Allegato H "Indicatori di Qualità".

2. Il Concessionario si impegna a collaborare, per quanto di propria competenza, con l'Amministrazione Utente, fornendo tempestivamente il supporto che si rendesse necessario, nell'ottica di garantire in buona fede l'efficiente conduzione delle attività di verifica di cui al comma precedente.

3. Le risultanze delle attività di verifica saranno comunicate al Direttore del Servizio del Concessionario perché siano eventualmente discusse in contraddittorio con il Direttore dell' Esecuzione e gli eventuali ulteriori rappresentanti dell'Amministrazione Utente, sia laddove si presentino delle criticità, perché si individuino in modo collaborativo le misure adatte al loro superamento, sia perché possano formare oggetto di conoscenza e miglioramento della *performance* laddove mettano in luce elementi positivi suscettibili di ulteriore implementazione o estensione.

## Articolo 14
## PROCEDURA DI CONTESTAZIONE DEI DISSERVIZI E PENALI

1. Fermo restando quanto previsto dagli artt. 21 e 23 della Convenzione, la ritardata, inadeguata o mancata prestazione dei Servizi a favore dell'Amministrazione Utente secondo quanto previsto dal presente Contratto comporta l'applicazione delle penali definite in termini oggettivi in relazione a quanto dettagliato all'Allegato H - "Indicatori di Qualità".

2. Il ritardato, inadeguato o mancato adempimento delle obbligazioni di cui al presente Contratto che siano poste a favore dell'Amministrazione Utente deve essere contestato al Direttore del Servizio.

3. La contestazione deve avvenire in forma scritta e motivata, con precisa quantificazione delle penali, nel termine di 8 (otto) giorni dal verificarsi del disservizio.

4. In caso di contestazione dell'inadempimento, il Concessionario dovrà comunicare per iscritto le proprie deduzioni, all'Amministrazione Utente entro 10 (dieci) giorni dalla ricezione della contestazione stessa. Laddove il Concessionario non contesti l'applicazione della penale a favore dell'Amministrazione Utente, il Concessionario provvederà, entro e non oltre 60 (sessanta) giorni, a corrispondere all'Amministrazione Utente la somma dovuta; decorso inutilmente il termine di cui al presente comma, l'Amministrazione Utente potrà provvedere ad incassare le garanzie nei limiti dell'entità della penale.

5. A fronte della contestazione della penale da parte dell'Amministrazione Utente, il Responsabile del Servizio e il Direttore dell'Esecuzione promuoveranno un tentativo di conciliazione, in seduta appositamente convocata dal Direttore dell'Esecuzione con la partecipazione dei rappresentanti del Concessionario di cui al precedente art. 5, lett. a. A fronte della mancata conciliazione, il Direttore dell'Esecuzione irrogherà la penale e, salvo lo spontaneo pagamento da parte del Concessionario, pur senza che ciò corrisponda ad acquiescenza, incamererà la garanzia entro i limiti della penale. Resta fermo il diritto del Concessionario di contestare la predetta penale iscrivendo riserva o agendo in giudizio per la restituzione.

6. La richiesta e/o il pagamento delle penali non esonera in nessun caso il Concessionario dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

## SEZIONE IV – GARANZIE E POLIZZE ASSICURATIVE

### Articolo 15
### GARANZIE

1. Fermo restando quanto previsto dall'art. 26 della Convenzione, le Parti danno atto che il Concessionario ha provveduto a costituire la garanzia definitiva con […], secondo lo schema tipo 1.2 del DM 19 gennaio 2018, n. 31 ("DM Garanzie").

2. Più in particolare, a garanzia delle obbligazioni contrattuali assunte nei confronti dell'Amministrazione Utente con la stipula del Contratto, il Concessionario ha prestato garanzia definitiva pari al 10% (dieci per cento) dell'importo del Contratto, salvo eventuali riduzioni di cui all'art. 103 del Codice, rilasciata in data _____ [•] dalla società _____ [•] avente numero [•]. _____ di importo pari ad Euro _____ [•] (_____/([•]/00).

3. La garanzia definitiva prestata in favore dell'Amministrazione Utente opera a far data dalla sottoscrizione del Contratto e dovrà avere validità almeno annuale da rinnovarsi, pena l'escussione, entro 30 (trenta) giorni dalla relativa scadenza per tutta la durata del Contratto stesso.

4. La garanzia prevista dal presente articolo cessa di avere efficacia dalla data di emissione del certificato di Verifica di Conformità o dell'attestazione, in qualunque forma, di regolare esecuzione delle prestazioni e viene progressivamente svincolata in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80% (ottanta per cento) dell'iniziale importo garantito, secondo quanto stabilito all'art. 103, comma 5, del Codice. Lo svincolo è automatico, senza necessità di nulla osta dell'Amministrazione Utente, con la sola condizione della preventiva consegna all'istituto garante, da parte del Concessionario, degli stati di avanzamento o di analogo documento, in originale o in copia autentica, attestanti l'avvenuta esecuzione. In ogni caso, lo

svincolo avverrà periodicamente con cadenza trimestrale a seguito della presentazione della necessaria documentazione all'Amministrazione Utente secondo quanto di competenza.

5. Laddove l'ammontare della garanzia prestata ai sensi del presente articolo dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Concessionario dovrà provvedere al reintegro entro il termine di 45 (quarantacinque) giorni lavorativi dal ricevimento della relativa richiesta effettuata dall'Amministrazione Utente, pena la risoluzione del Contratto.

6. La garanzia prestata ai sensi del presente articolo è reintegrata dal Concessionario a fronte dell'ampliamento del valore dei Servizi dedotti in Contratto nel corso dell'efficacia di questo, ovvero nel caso di estensione della durata della Convenzione e/o del Contratto ai sensi dell'art. 4, comma 2 del Contratto.

## Articolo 16
## POLIZZE ASSICURATIVE

1. Fermo restando quanto previsto dall'art. 27 della Convenzione, il Concessionario si impegna a stipulare idonee polizze assicurative, conformi allo schema tipo 1.2 del DM Garanzie a copertura delle attività oggetto del Contratto.

2. In particolare, ferme restando le coperture assicurative previste per legge in capo agli eventuali professionisti di cui il Concessionario si può avvalere nell'ambito della Concessione, il Concessionario ha l'obbligo di stipulare una polizza assicurativa a favore dell'Amministrazione Utente, a copertura dei danni che possano derivare dalla prestazione dei Servizi, con validità ed efficacia a far data dalla sottoscrizione del Contratto, prima dell'avvio del Servizio ai sensi dell'art. 8 del Contratto, nonché, in caso di utilizzo del servizio di *housing*, una polizza a copertura dei danni materiali direttamente causati alle cose assicurate (c.d. All Risks), per tutta la durata del Contratto, che non escluda eventi quali incendio e furto.

## Articolo 17
## GARANZIE DEL CONCESSIONARIO PER I FINANZIATORI

1. Fermo restando quanto previsto dall'art. 28 della Convenzione, l'Amministrazione Utente prende atto ed accetta sin d'ora l'eventuale costituzione da parte del Concessionario in favore dei Finanziatori, di pegni su azioni del Concessionario e di garanzie sui crediti che verranno a maturazione in forza del presente Contratto.

2. In ogni caso, da tale accettazione non potranno derivare a carico dell'Amministrazione Utente nuovi o maggiori oneri rispetto a quelli derivanti dal presente Contratto e, con riferimento alla cessione dei, ovvero al pegno sui, crediti, l'Amministrazione Utente potrà opporre al cessionario/creditore pignoratizio tutte le eccezioni opponibili al Concessionario in base al Contratto.

3. L'Amministrazione Utente si impegna a cooperare, per quanto di propria competenza, affinché siano sottoscritti i documenti necessari a garantire il perfezionamento e/o l'opponibilità, ove necessario, delle garanzie costituire a favore dei Finanziatori, inclusi a mero titolo esemplificativo eventuali atti di accettazione della cessione dei, o del pegno sui, crediti derivanti dal Contratto.

4. In ogni caso, il Concessionario si impegna a far sì che eventuali cessioni del credito siano disposte solo *pro-soluto* e subordinatamente all'accettazione dell'Amministrazione Utente, ove sia debitore ceduto.

## SEZIONE V – VICENDE DEL CONTRATTO

### Articolo 18
### EFFICACIA DEL CONTRATTO

1. Il Contratto assume efficacia per il Concessionario dalla data di sua sottoscrizione, per l'Amministrazione Utente dalla data della registrazione, se prevista.

### Articolo 19
### RISOLUZIONE PER INADEMPIMENTO DEL CONCESSIONARIO

1. Fermo restando quanto previsto dall'art. 33 della Convenzione, l'Amministrazione Utente può dar luogo alla risoluzione del Contratto, previa diffida ad adempiere, ai sensi dell'art. 1454 Cod. Civ., comunicata per iscritto al Concessionario, ai sensi dell'art. 23 del Contratto, con l'attribuzione di un termine per l'adempimento ragionevole e, comunque, non inferiore a giorni 60 (sessanta), nei seguenti casi:

   a) riscontro di gravi vizi nella gestione del Servizio;

   b) applicazione di penali, ai sensi dell'art. 15 del Contratto, per un importo che supera il 10% (dieci per cento) del valore del Contratto;

   c) nel caso di mancato reintegro della garanzia ove si verifichi la fattispecie di cui all'art. 15, commi 5 e 6 del presente Contratto.

2. In caso di risoluzione per inadempimento del Concessionario, a quest'ultimo sarà dovuto il pagamento delle prestazioni regolarmente eseguite e delle spese eventualmente sostenute la predisposizione, *set-up*, messa a disposizione o ammodernamento dell'Infrastruttura, decurtato degli oneri aggiuntivi derivanti dallo scioglimento del Contratto.

### Articolo 20
### REVOCA E RISOLUZIONE PER INADEMPIMENTO DELL'AMMINISTRAZIONE UTENTE

1. Fermo restando quanto previsto dall'art. 35 della Convenzione, l'Amministrazione Utente può disporre la revoca dell'affidamento in concessione dei Servizi oggetto del Contratto solo per inderogabili e giustificati motivi di pubblico interesse, che debbono essere adeguatamente motivati e comprovati, con contestuale comunicazione al Concessionario, con le modalità di cui all'art. 23 del Contratto. In tal caso, l'Amministrazione Utente deve corrispondere al Concessionario le somme di cui al comma 2 del presente articolo.

2. Qualora il Contratto sia risolto per inadempimento dell'Amministrazione Utente, non imputabile al Concessionario, ovvero sia disposta la revoca di cui al comma precedente, l'Amministrazione Utente è tenuta a provvedere al pagamento, ai sensi dell'art. 176, commi 4 e 5 del Codice, in favore del Concessionario:

   a) degli importi eventualmente maturati dal Concessionario ai sensi del Contratto;

   b) dei costi sostenuti per lo svolgimento delle prestazioni eseguite;

c) dei costi sostenuti per la produzione di Servizi non ancora interamente prestati o non pagati;

d) dei costi e delle penali da sostenere nei confronti di terzi, in conseguenza della risoluzione;

e) dell'indennizzo a titolo di risarcimento del mancato guadagno, pari al 10% (dieci per cento), del valore dei Servizi ancora da prestare;

3. L'efficacia della risoluzione e della revoca di cui al comma 1 del presente articolo resta in ogni caso subordinata all'effettivo integrale pagamento degli importi previsti al comma 2 da parte dell'Amministrazione Utente.

4. L'efficacia della risoluzione del Contratto non si estende alle prestazioni già eseguite ai sensi dell'art. 1458 Cod. Civ., rispetto alle quali il Concedente e l'Amministrazione Utente sono tenuti al pagamento per intero dei relativi importi.

5. Al fine di quantificare gli importi di cui al comma 2 del presente articolo, l'Amministrazione Utente, in contraddittorio con il Concessionario e alla presenza del Direttore del Servizio, redige apposito verbale, entro 30 (trenta) giorni successivi alla ricezione, da parte del Concessionario, del provvedimento di revoca ovvero alla data della risoluzione. Qualora tutti i soggetti coinvolti siglino tale verbale senza riserve e/o contestazioni, i fatti e dati registrati si intendono definitivamente accertati, e le somme dovute al Concessionario devono essere corrisposte entro i 30 (trenta) giorni successivi alla compilazione del verbale. In caso di mancata sottoscrizione la determinazione è rimessa all'arbitraggio di un terzo nominato dal Presidente del Tribunale di Roma.

6. Senza pregiudizio per il pagamento delle somme di cui al comma 2 del presente articolo, in tutti i casi di cessazione del Contratto diversi dalla risoluzione per inadempimento del Concessionario, quest'ultimo ha il diritto di proseguire nella gestione ordinaria dei Servizi, incassando il relativo corrispettivo, sino all'effettivo pagamento delle suddette somme.

7. Per tutto quanto non specificato nel presente articolo, si rinvia integralmente all'art. 176 del Codice.

## Articolo 21
## RECESSO

1. Fermo restando quanto previsto dall'art. 36 della Convenzione, in caso di sospensione del Servizio per cause di Forza Maggiore, ai sensi dell'art. 19 della Convenzione, protratta per più di 90 (novanta) giorni, ciascuna delle Parti può esercitare il diritto di recedere dal Contratto.

2. Nei casi di cui al comma precedente, l'Amministrazione Utente deve, prontamente e in ogni caso entro 30 (trenta) giorni, corrispondere al Concessionario l'importo di cui all'art. 20, comma 2 del Contratto, con l'esclusione, ai sensi di quanto previsto dall'art. 165, comma 6 del Codice, degli importi di cui alla lettera c) di cui al citato art. 20, comma 2 del Contratto.

3. Nelle more dell'individuazione di un subentrante, il Concessionario dovrà proseguire sempreché sia economicamente sostenibile, laddove richiesto dall'Amministrazione Utente, nella prestazione dei Servizi, alle medesime modalità e condizioni del Contratto, con applicazione delle previsioni di cui all'art. 5 della Convenzione in relazione ad eventuali investimenti e, comunque, a fronte dell'effettivo pagamento dell'importo di cui all'art. 20, comma 2 del Contratto.

4. Inoltre, fermo restando quanto previsto al precedente comma del presente articolo, il

Concessionario può chiedere all'Amministrazione Utente di continuare a gestire il Servizio alle medesime modalità e condizioni del Contratto, fino alla data dell'effettivo pagamento delle somme di cui al comma 2 del presente articolo.

**Articolo 22**
**SCADENZA DEL CONTRATTO**

1. Alla scadenza del Contratto, il Concessionario ha l'obbligo di facilitare in buona fede la migrazione dell'Amministrazione Utente verso il nuovo concessionario nella gestione dei Servizi o comunque verso l'eventuale diversa soluzione che sarà individuata dall'Amministrazione Utente, ferma restando la tutela dei suoi diritti e interessi legittimi.

## SEZIONE VI – ULTERIORI DISPOSIZIONI

**Articolo 23**
**COMUNICAZIONI**

1. Agli effetti del Contratto, il Concessionario elegge domicilio in [•], l'Amministrazione Utente elegge domicilio in [•].

2. Eventuali modifiche del suddetto domicilio devono essere comunicate per iscritto e hanno effetto a decorrere dall'intervenuta ricezione della relativa comunicazione.

3. Tutte le comunicazioni previste dalla Convenzione devono essere inviate in forma scritta a mezzo lettera raccomandata A.R. oppure via PEC ai seguenti indirizzi:

   [•]

4. Le predette comunicazioni sono efficaci dal momento della loro ricezione da parte del destinatario, certificata dall'avviso di ricevimento, nel caso della lettera raccomandata A.R., ovvero, nel caso di invio tramite PEC, dalla relativa ricevuta.

**Articolo 24**
**NORME ANTICORRUZIONE E ANTIMAFIA, PROTOCOLLI DI LEGALITÀ**

1. Il Concessionario, con la sottoscrizione del Contratto, attesta, ai sensi e per gli effetti dell'art. 53, comma 16-ter del Codice antimafia, di non aver concluso contratti di lavoro subordinato o autonomo o, comunque, aventi ad oggetto incarichi professionali con ex dipendenti del DTD, che abbiano esercitato poteri autoritativi o negoziali per conto dello stesso DTD nei confronti del medesimo Concessionario, nel triennio successivo alla cessazione del rapporto di pubblico impiego.

2. [**eventuale**: Il Concessionario, con riferimento alle prestazioni oggetto del Contratto, si impegna - ai sensi dell'art. [•] del Codice di comportamento/Protocollo di legalità [•] - ad osservare e a far osservare ai propri collaboratori a qualsiasi titolo, per quanto compatibili con il ruolo e l'attività svolta, gli obblighi di condotta previsti dal Codice di comportamento/Protocollo stesso.

3. A tal fine, il Concessionario dà atto che l'Amministrazione Utente ha provveduto a trasmettere, ai sensi dell'art. [•] del Codice di comportamento/Protocollo di legalità sopra richiamato, copia del Codice/Protocollo stesso per una sua più completa e piena conoscenza. Il Concessionario si impegna a trasmettere copia dello stesso ai propri collaboratori a qualsiasi titolo.]

4. La violazione degli obblighi, di cui al presente articolo, costituisce causa di risoluzione del Contratto.

**Articolo 25**
**OBBLIGHI IN TEMA DI TRACCIABILITÀ DEI FLUSSI FINANZIARI**

1. Il Concessionario assume tutti gli obblighi di tracciabilità dei flussi finanziari, per sé e per i propri subcontraenti, di cui all'art. 3, legge 13 agosto 2010, n. 136 e ss.mm.ii., dandosi atto che, nel caso di inadempimento, il Contratto si risolverà di diritto, *ex* art. 1456 Cod. Civ..

**Articolo 26**
**CONTROVERSIE E FORO COMPETENTE**

1. Per tutte le controversie che dovessero insorgere nell'esecuzione del presente Contratto è competente in via esclusiva l'Autorità Giudiziaria di Roma.

**Articolo 27**
**TRATTAMENTO DEI DATI PERSONALI**

1. In materia di trattamento dei dati personali, si rinvia alla Normativa Privacy e al GDPR, come vigenti, e ai relativi obblighi per il Concessionario, descritti nell'Allegato E "Facsimile nomina Responsabile trattamento dei dati personali" che opportunamente compilato e firmato per accettazione della nomina dal Concessionario diventa parte integrante del presente Contratto.

**Articolo 28**
**REGISTRAZIONE**

1. La stipula del Contratto è soggetta a registrazione. Tutte le spese dipendenti dalla stipula del Contratto sono a carico del Concessionario.

**Articolo 29**
**RINVIO AL CODICE CIVILE E AD ALTRE DISPOSIZIONI DI LEGGE VIGENTI**

1. Per quanto non espressamente disciplinato dal Contratto, trovano applicazione le disposizioni normative di cui al Cod. Civ., e le altre disposizioni normative e regolamentari applicabili in materia.

2. Oltre all'osservanza di tutte le norme specificate nel Contratto, il Concessionario ha l'obbligo di osservare tutte le disposizioni contenute in leggi, o regolamenti, in vigore o che siano emanati durante il corso della Concessione, di volta in volta applicabili.

---

**(……)**

---

**(……)**

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della
Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1
dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO E

## FACSIMILE

### NOMINA RESPONSABILE TRATTAMENTO DEI DATI PERSONALI

***<<Valuti la PA se valorizzare diversamente i riferimenti al Titolare, al Responsabile, al sub Responsabile, ai terzi autorizzati al Trattamento, in ragione della propria specifica posizione. >>***

## NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI

1. Con la sottoscrizione della presente da parte dell'Amministrazione [⚫] il Concessionario è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche *"Regolamento UE"*), per tutta la durata del Contratto di Utenza (nel seguito anche "Contratto") relativo alla "*Concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012*". A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto dell'Amministrazione (Titolare del Trattamento), **le sole operazioni di trattamento necessarie per fornire il servizio oggetto del Contratto e della Convenzione**, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE 2016/679, del D.Lgs. 196/2003 e s.m.i e del D. Lgs. n. 101/2018 (nel seguito anche *"Normativa in tema di trattamento dei dati personali"*), e delle istruzioni nel seguito fornite.

2. Il Concessionario/Responsabile si impegna a presentare su richiesta dell'Amministrazione garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

3. Le finalità del trattamento sono: ***<<Valorizzare in ragione dell'oggetto del contratto__>>***

4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: ***<<Valorizzare in ragione dell'oggetto del contratto*** i) dati personali (es. dati anagrafici e di contatto ecc.); ii) categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE c.d. sensibili; iii) dati personali relativi a condanne penali e reati di cui all'art. 10 del Regolamento UE c.d. giudiziari**>>**.

5. Le categorie di interessati sono: ***<<Valorizzare in ragione dell'oggetto del contratto*** es. dipendenti e collaboratori, utenti dei servizi, ecc.**>>**.

6. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

   a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

   b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

   c) trattare i dati personali conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Concessionario si impegna a far osservare anche alle persone da questi

autorizzate ad effettuare il trattamento dei dati personali oggetto del presente Contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Concessionario deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell'ambito del presente Contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente Contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - ricevano la formazione necessaria in materia di protezione dei dati personali;
   - trattino i dati personali osservando le istruzioni impartite dal Titolare al Responsabile;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta>;

i) adottare le misure minime di sicurezza ICT per le PP.AA. ***<specificare il livello richiesto>***.

7. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Concessionario si impegna a fornire all'Amministrazione un piano di misure di sicurezza rimesse all'approvazione della stessa, che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso ***<<personalizzare in ragione dell'oggetto del Contratto>>***:

   - la pseudonimizzazione e la cifratura dei dati personali;
   - la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

8. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

   A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre ***<<o diverso termine indicato dalla PA>>*** giorni lavorativi; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Concessionario agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il Concessionario ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. ***1) (Autorizzazione generale)*** Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente [⚫]***<<la PA deve specificare la periodicità>>***, il Titolare del trattamento delle nomine e delle sostituzioni dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei sub-Responsabili nominati e i dati del contratto di esternalizzazione. ***<<Oppure>> 2) (Autorizzazione specifica)*** Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.

10. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub- Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

    Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il

Concessionario/Responsabile Iniziale del trattamento a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ***<<selezionare una tra le due opzioni: 1.*** ad informare tempestivamente il Titolare del trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del trattamento, nei termini previsti dalla Regolamento UE; ***oppure 2.***ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti **>>**

12. Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile ***<<da valorizzare in alternativa***: sub-Responsabile**>>** del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.

14. Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Concessionario/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

15. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile, su richiesta del Titolare, si impegna a: *i)* restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; *ii)* distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

16. Il Concessionario si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.

17. Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali, trattati in esecuzione del contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

18. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione

internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

19. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

20. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

21. Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuta nella Convezione (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori.

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO F

## PIANO ECONOMICO FINANZIARIO
### ASSEVERATO E COMPRENSIVO DELLA
### RELAZIONE ILLUSTRATIVA

## Oggetto dell'Allegato

Il presente allegato è costituito dai seguenti annessi:

- Annesso 1: Piano economico finanziario asseverato;
- Annesso 2: Relazione illustrativa.

DTD-0003947-A-24/08/2022 - Allegato Utente 4 (A04)



Spett.le

**Polo Strategico Nazionale S.p.A.**

Via Goito, 4

00185 Roma

Oggetto: Lettera di asseverazione del piano economico – finanziario (PEF), concernente l'intervento relativo alla progettazione, realizzazione, messa a disposizione e gestione – in regime di concessione ed in condizioni di equilibrio economico finanziario - dei servizi infrastrutturali e applicativi *in cloud* per la gestione di dati sensibili "Polo Strategico Nazionale" (PSN) (il "**Progetto**"), da affidarsi mediante procedura di finanza di progetto ai sensi dell'articolo 183 (*Finanza di progetto*), comma quindici del Decreto Legislativo 18 aprile 2016 n. 50 e s.m.i.

Gentili Signori,

facciamo riferimento al Progetto distinto in oggetto, nonché alla documentazione ed ai dati che sono stati al riguardo forniti da parte Vostra.

Al riguardo, in esecuzione dell'incarico conferito, Hermes Asseverazioni S.r.l. ("**Hermes**")

**ASSEVERA**

ai sensi e per gli effetti dell'art.183 (*Finanza di progetto*) e seguenti del D.lgs. 50/2016 e dell'art. 96 (*Requisiti del proponente e attività di asseverazione*) del D.P.R. 5 ottobre 2010, n. 207 e successive modifiche ed integrazioni il piano economico e finanziario predisposto dalla Vostra società o per il tramite di essa al costituendo ATI, che si allega alla presente, attestandone la coerenza nel suo complesso sulla base, tra l'altro, dei seguenti elementi:

**Sede legale e amministrativa**
Via Ermete Novelli 1 - 40127 Bologna
P.IVA e Cod. Fisc. 03514851207 – Capitale Sociale € 10.000,00 iv
Tel 051 375341 - Fax 051 6569142
E-mail hermesasseverazionisrl@gmail.com
Pec: hermesasseverazionisrl@legalmail.it
Sito web: www.hermesrevisione.it

(a) struttura finanziaria dell'operazione, comprensiva dell'analisi dei profili di bancabilità dell'operazione in relazione alle fonti di debito indicate nel PEF;

(b) costi, ricavi e conseguenti flussi di cassa generati dal Progetto.

A causa dell'aleatorietà connessa alla realizzazione di eventi futuri, non possono escludersi scostamenti anche significativi fra i valori consuntivi e valori preventivati nel Piano.

Ove occorre, Hermes ricorda che il piano economico finanziario è stato predisposto da parte della Vostra Società o per il tramite di essa dal costituendo ATI, direttamente o avvalendosi di consulenti esterni. Pertanto, la responsabilità della redazione del piano economico finanziario nonché delle ipotesi e degli elementi posti alla base della sua formulazione, resta in capo alla Vostra Società o per il tramite di essa al costituendo ATI.

Nello svolgimento dell'attività di cui sopra, Hermes si è basata su dati e documentazione relativi al Progetto forniti da parte dei soggetti proponenti.

I soggetti proponenti si assumono pertanto ogni responsabilità circa la veridicità e congruità dei suddetti dati e documenti nonché, più in generale, di qualsiasi altra informazione comunicataci ai fini della redazione della presente lettera di asseverazione.

La presente lettera di asseverazione viene resa a beneficio e nell'interesse dei soggetti proponenti, con l'espresso avvertimento che:

1. Hermes non svolge, nell'ambito del rilascio della presente lettera di asseverazione, alcuna funzione di natura pubblica; e
2. la presente lettera di asseverazione non costituisce (né può essere interpretata quale) attività sostitutiva della funzione di verifica e valutazione della proposta, di competenza della amministrazione aggiudicatrice.

La presente lettera di asseverazione è stata predisposta su incarico della società in indirizzo.

**Sede legale e amministrativa**
Via Ermete Novelli 1 - 40127 Bologna
P.IVA e Cod. Fisc. 03514851207 – Capitale Sociale € 10.000,00 iv
Tel 051 375341 - Fax 051 6569142
E-mail hermesasseverazionisrl@gmail.com
Pec: hermesasseverazionisrl@legalmail.it
Sito web: www.hermesrevisione.it

Essa viene rilasciata e potrà essere pertanto liberamente divulgata da parte di questi ultimi nel contesto della presentazione relativa al Progetto e della sua valutazione da parte delle amministrazioni interessate e/o altrimenti competenti in ogni fase della relativa procedura. Al di fuori di tali ipotesi, e fatti salvi i casi altrimenti previsti ai sensi delle applicabili disposizioni di legge e/o ove altrimenti richiesto da parte di qualsiasi Autorità competente, essa non potrà essere resa nota a terzi senza il nostro preventivo consenso scritto.

Distinti saluti.

**Hermes Asseverazioni S.r.l.**
**Dott. Dario Rossi**
Partner

HERMES ASSEVERAZIONI SRL
Via Ermete Novelli, 1
40127 Bologna
P. IVA e C.F. 03514851207

Bologna, 22 agosto 2022

Elenco allegati:

- Piano Economico Finanziario

**Sede legale e amministrativa**
Via Ermete Novelli 1 - 40127 Bologna
P.IVA e Cod. Fisc. 03514851207 – Capitale Sociale € 10.000,00 iv
Tel 051 375341 - Fax 051 6569142
E-mail hermesasseverazionisrl@gmail.com
Pec: hermesasseverazionisrl@legalmail.it
Sito web: www.hermesrevisione.it

**Tabella 1: Piano Economico Finanziario - Calcolo Indici**

| | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **TIR di Progetto** | | | | | | | | | | | | | | | |
| Valore iniziale degli asset | | | | | | | | | | | | | | | |
| Flusso di liquidità della gestione operativa | | (88,6) | (44,2) | (45,5) | (71,6) | 6,4 | 16,6 | 27,3 | 30,3 | 46,3 | 62,1 | 73,4 | 68,9 | 52,6 | 15,8 |
| Rettifica Fabbisogno IVA | | (24,1) | (10,5) | (11,1) | (16,6) | 12,2 | (6,8) | 8,3 | (6,8) | 0,6 | 0,7 | 1,6 | 8,0 | 10,3 | 34,1 |
| Rettifica oneri/proventi finanziari (finanziamenti) | | 3,1 | 5,0 | 6,0 | 6,7 | 7,9 | 7,9 | 7,9 | 7,6 | 7,3 | 6,3 | 4,8 | 3,2 | 2,3 | 0,6 |
| *Rettifica variazione CCN* | | | | | | | | | | | | | | | 1,8 |
| Valore finale degli asset | | | | | | | | | | | | | | | |
| **Totale flussi di cassa, lordo imposte** | - | **(109,7)** | **(49,7)** | **(50,5)** | **(81,5)** | **26,5** | **17,7** | **43,6** | **31,0** | **54,2** | **69,2** | **79,8** | **80,1** | **65,2** | **52,3** |
| **Tasso Interno di Rendimento di progetto, lordo imposte** | 7,7% | | | | | | | | | | | | | | |
| Imposte sul reddito di esercizio | | - | - | - | - | (0,7) | (2,3) | (6,7) | (8,8) | (12,4) | (15,5) | (16,8) | (14,1) | (10,2) | - |
| **Totale flussi di cassa, netto imposte** | - | **(109,7)** | **(49,7)** | **(50,5)** | **(81,5)** | **25,8** | **15,4** | **36,9** | **22,3** | **41,8** | **53,7** | **63,0** | **66,0** | **55,0** | **52,3** |
| **Tasso Interno di Rendimento di progetto, netto imposte** | 5,1% | | | | | | | | | | | | | | |
| **TIR dell'azionista** | | | | | | | | | | | | | | | |
| Apporto azionisti | | (29,0) | (28,3) | (22,8) | (25,1) | - | - | - | (0,0) | - | - | - | - | - | - |
| Dividendi, Rimborso riserva versamento soci, Utili portati a nuovo | | - | - | - | - | 13,0 | - | 10,9 | 16,0 | 9,6 | 18,0 | 18,0 | 60,5 | 43,1 | 15,8 |
| Patrimonio netto fine concessione | | | | | | | | | | | | | | | 1,8 |
| Flussi all'azionista | | (29,0) | (28,3) | (22,8) | (25,1) | 13,0 | - | 10,9 | 16,0 | 9,6 | 18,0 | 18,0 | 60,5 | 43,1 | 17,5 |
| **TIR dell'Azionista** | 8,4% | | | | | | | | | | | | | | |
| **DSCR** | | | | | | | | | | | | | | | |
| *Check Anno Calcolo DSCR* | | *0,0* | *0,0* | *0,0* | *0,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *0,0* | *0,0* |
| Flusso di cassa disponibile per il servizio del debito | | (18,5) | (9,5) | (8,9) | (13,4) | 14,2 | 24,1 | 34,2 | 36,1 | 50,0 | 63,1 | 63,0 | 59,1 | 45,4 | 16,4 |
| Servizio del Debito | | 3,1 | 5,0 | 6,0 | 6,7 | 10,1 | 17,2 | 24,4 | 25,8 | 35,7 | 45,1 | 45,0 | 21,1 | 2,3 | 0,6 |
| **DSCR** | | n.a. | n.a. | n.a. | n.a. | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 2,80 | n.a. | n.a. |
| Finanziamento Outstanding BoP | | 128,9 | 157,7 | 185,0 | 230,7 | 222,5 | 207,1 | 184,3 | 159,7 | 124,7 | 79,2 | 32,2 | 7,2 | - | - |
| **DSCR medio ponderato** | 1,41x | | | | | | | | | | | | | | |
| **DSCR minimo** | 1,40 | | | | | | | | | | | | | | |
| **LLCR** | | | | | | | | | | | | | | | |
| *Check Anno Calcolo LLCR* | | *0,0* | *0,0* | *0,0* | *0,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *1,0* | *0,0* | *0,0* |
| Debito Outstanding Inizio Periodo | | 128,9 | 157,7 | 185,0 | 230,7 | 222,5 | 207,1 | 184,3 | 159,7 | 124,7 | 79,2 | 32,2 | 7,2 | - | - |
| Interessi di periodo | | 3,1 | 5,0 | 6,0 | 6,7 | 7,9 | 7,9 | 7,9 | 7,6 | 7,3 | 6,3 | 4,8 | 3,2 | 2,3 | 0,6 |
| Costo Medio del Debito di periodo | | 3,4% | 3,5% | 3,5% | 3,6% | 3,6% | 3,6% | 3,6% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% |
| Flusso di Cassa Disponibile per Rimborso del Debito | | (18,5) | (9,5) | (8,9) | (13,4) | 14,2 | 24,1 | 34,2 | 36,1 | 50,0 | 63,1 | 63,0 | 59,1 | 45,4 | 16,4 |
| Flussi di Cassa Attualizzati | | n.a. | n.a. | n.a. | n.a. | 329,7 | 326,9 | 314,2 | 291,2 | 265,6 | 225,3 | 170,6 | 113,9 | n.a. | n.a. |
| **LLCR** | | n.a. | n.a. | n.a. | n.a. | 1,48 | 1,58 | 1,70 | 1,82 | 2,13 | 2,85 | 5,30 | 15,79 | n.a. | n.a. |
| **LLCR medio ponderato** | 2x | | | | | | | | | | | | | | |
| **LLCR minimo** | 1,48 | | | | | | | | | | | | | | |

HERMES ASSEVERAZIONI SRL
Via Ermete Novelli, 1
40127 Bologna
P. IVA e C.F. 03514851207

**Tabella 2: Piano Economico Finanziario - Conto Economico**

| | Totale | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ricavi** | | | | | | | | | | | | | | | | |
| Housing | **79,9** | | 0,4 | 1,6 | 3,9 | 6,5 | 8,1 | 8,1 | 8,0 | 8,0 | 8,1 | 8,1 | 7,8 | 6,6 | 4,8 | - |
| Hosting | **336,1** | | 1,5 | 6,3 | 15,2 | 25,5 | 32,0 | 32,7 | 33,1 | 33,7 | 34,8 | 35,8 | 34,7 | 29,2 | 21,4 | - |
| IaaS Private | **327,5** | | 1,4 | 5,9 | 14,3 | 23,9 | 30,1 | 31,2 | 31,8 | 32,8 | 34,2 | 35,5 | 34,6 | 29,1 | 22,5 | - |
| IaaS Shared | **305,3** | | 1,3 | 5,5 | 13,3 | 22,3 | 28,1 | 29,0 | 29,7 | 30,6 | 31,9 | 33,1 | 32,3 | 27,2 | 21,0 | - |
| Altri servizi di IaaS e Cloud | **233,0** | | 0,9 | 3,8 | 9,2 | 15,6 | 19,9 | 21,1 | 22,4 | 23,8 | 25,2 | 26,8 | 26,3 | 22,0 | 15,9 | - |
| Hybrid Cloud on PSN Site | **232,0** | | - | - | - | 2,1 | 5,4 | 11,3 | 20,2 | 28,0 | 33,2 | 39,9 | 41,0 | 33,0 | 17,8 | - |
| Public Cloud PSN Managed | **252,1** | | - | - | - | 2,3 | 5,9 | 12,3 | 22,0 | 30,5 | 36,1 | 43,4 | 44,5 | 35,9 | 19,4 | - |
| Secure Public Cloud | **556,8** | | 2,0 | 8,3 | 19,9 | 33,9 | 43,5 | 46,4 | 49,7 | 53,1 | 56,5 | 60,1 | 61,9 | 61,4 | 60,2 | - |
| PaaS Industry | **57,2** | | - | 5,4 | 5,5 | 5,6 | 5,6 | 5,7 | 5,8 | 5,8 | 5,9 | 5,9 | 6,0 | - | - | - |
| Sistemi operativi | **128,8** | | 0,6 | 2,3 | 5,6 | 9,4 | 11,9 | 12,2 | 12,5 | 12,9 | 13,5 | 14,0 | 13,6 | 11,5 | 8,9 | - |
| Ricavi da migrazione | **147,4** | | 12,7 | 28,8 | 29,1 | 58,0 | 0,4 | 0,9 | 1,6 | 2,3 | 2,7 | 3,2 | 3,3 | 2,7 | 1,5 | - |
| **Ricavi da servizi core** | **2.656,2** | **-** | **21,0** | **68,0** | **116,0** | **205,2** | **191,1** | **211,1** | **236,9** | **261,4** | **282,0** | **305,8** | **305,9** | **258,5** | **193,4** | **-** |
| Professional Services | **76,5** | | 0,5 | 1,9 | 4,5 | 6,6 | 6,7 | 6,8 | 6,9 | 6,9 | 7,0 | 7,1 | 7,1 | 7,2 | 7,3 | - |
| Rearchitect | **184,8** | | 14,3 | 32,2 | 32,6 | 38,4 | 33,4 | 34,0 | - | - | - | - | - | - | - | - |
| Replatform | **91,8** | | 7,1 | 16,0 | 16,2 | 19,1 | 16,6 | 16,9 | - | - | - | - | - | - | - | - |
| Business & Culture Enablement | **27,6** | | 0,3 | 1,0 | 2,3 | 2,9 | 2,4 | 2,4 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,1 | 1,6 | - |
| IT infrastructure - service operations | **32,7** | | 0,1 | 0,6 | 1,3 | 2,3 | 2,9 | 3,0 | 3,1 | 3,3 | 3,5 | 3,6 | 3,6 | 3,0 | 2,3 | - |
| **Totale Ricavi** | 3.069,49 | | **43,2** | **119,7** | **173,0** | **274,4** | **253,0** | **274,2** | **249,3** | **274,1** | **295,0** | **319,0** | **319,1** | **270,9** | **204,7** | **-** |

HERMES ASSICURAZIONI SRL
Via Ermete Zavarelli, 1
40122 Bologna
P. IVA e C.F. 03514851207

**Tabella 2: Piano Economico Finanziario - Conto Economico**

| | Totale | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Costi Operativi** | | | | | | | | | | | | | | | | |
| **Costi diretti** | **(2.293,7)** | | **(48,3)** | **(118,7)** | **(154,4)** | **(234,4)** | **(200,2)** | **(215,2)** | **(175,8)** | **(193,9)** | **(202,6)** | **(216,1)** | **(213,8)** | **(181,8)** | **(138,4)** | - |
| Connettività | **(65,9)** | | (1,3) | (2,1) | (3,5) | (5,0) | (6,0) | (6,1) | (6,2) | (6,3) | (6,5) | (6,6) | (6,4) | (5,5) | (4,4) | - |
| Spazi attrezzati (esclusi canoni di affitto) | **(55,0)** | | (1,2) | (1,8) | (3,3) | (5,7) | (5,1) | (5,1) | (5,1) | (5,2) | (5,2) | (5,3) | (5,0) | (4,1) | (3,0) | - |
| Energia | **(105,1)** | | (1,2) | (2,9) | (6,1) | (8,3) | (10,1) | (10,2) | (10,1) | (10,1) | (10,3) | (10,5) | (10,1) | (8,5) | (6,4) | - |
| Sicurezza | **(47,1)** | | (0,2) | (0,9) | (2,2) | (3,7) | (4,6) | (4,7) | (4,7) | (4,7) | (4,8) | (4,9) | (4,7) | (3,9) | (2,9) | - |
| Manutenzioni | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Software | **(306,0)** | | (1,5) | (6,1) | (14,5) | (23,8) | (29,4) | (33,6) | (30,1) | (30,5) | (31,2) | (31,8) | (30,3) | (24,9) | (18,5) | - |
| Ops tecniche INT | **(32,1)** | | (1,6) | (2,1) | (3,0) | (2,5) | (2,5) | (2,6) | (2,6) | (2,7) | (2,8) | (2,8) | (2,8) | (2,4) | (1,8) | - |
| Ops tecniche EXT | **(12,9)** | | (0,9) | (0,9) | (1,1) | (1,0) | (1,0) | (1,0) | (1,0) | (1,1) | (1,1) | (1,1) | (1,1) | (0,9) | (0,7) | - |
| LAN & WAN Management | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Security Operations (SOC + servizi prof.) | **(96,9)** | | (2,5) | (2,7) | (5,7) | (8,7) | (9,2) | (9,0) | (9,0) | (9,1) | (9,3) | (9,4) | (9,0) | (7,5) | (5,7) | - |
| Sicurezza (CERT) | **(6,5)** | | (0,1) | (0,2) | (0,3) | (0,6) | (0,6) | (0,6) | (0,6) | (0,7) | (0,7) | (0,7) | (0,6) | (0,5) | (0,3) | - |
| Controllo Produzione IT | **(96,9)** | | (0,5) | (1,5) | (3,8) | (6,8) | (8,5) | (9,0) | (9,3) | (9,8) | (10,3) | (10,9) | (10,7) | (9,0) | (6,7) | - |
| COPS | **(98,8)** | | (0,3) | (1,6) | (3,9) | (6,8) | (9,0) | (9,3) | (9,6) | (9,9) | (10,5) | (10,9) | (10,8) | (9,1) | (6,9) | - |
| Service management | **(21,0)** | | (0,1) | (0,3) | (0,8) | (1,4) | (1,9) | (2,0) | (2,1) | (2,1) | (2,2) | (2,3) | (2,3) | (2,0) | (1,5) | - |
| IT infrastructure - service operations | **(33,3)** | | (0,1) | (0,5) | (1,3) | (2,3) | (2,9) | (3,0) | (3,2) | (3,4) | (3,5) | (3,7) | (3,7) | (3,2) | (2,4) | - |
| Servizi professionali di sicurezza | **(77,9)** | | (0,4) | (1,8) | (4,5) | (6,6) | (6,7) | (6,8) | (6,9) | (7,1) | (7,2) | (7,3) | (7,4) | (7,5) | (7,6) | - |
| Secure Public Cloud (quota PSN) | **(47,9)** | | (1,0) | (1,1) | (1,7) | (2,2) | (3,9) | (4,7) | (4,3) | (4,9) | (4,9) | (5,1) | (5,0) | (4,7) | (4,3) | - |
| Rearchitect | **(182,7)** | | (13,8) | (31,4) | (32,1) | (38,0) | (33,3) | (34,1) | - | - | - | - | - | - | - | - |
| Replatform | **(90,7)** | | (6,8) | (15,6) | (15,9) | (18,9) | (16,5) | (16,9) | - | - | - | - | - | - | - | - |
| Business & Culture Enablement | **(29,8)** | | (0,3) | (1,2) | (2,7) | (3,3) | (2,5) | (2,5) | (2,6) | (2,6) | (2,7) | (2,7) | (2,7) | (2,3) | (1,8) | - |
| Public Cloud PSN Managed (quota PSN) | **(41,2)** | | (0,6) | (1,1) | (1,1) | (0,4) | (1,1) | (2,1) | (3,7) | (4,9) | (5,6) | (6,5) | (6,5) | (5,1) | (2,6) | - |
| Secure Public Cloud (rivendita CSP) | **(379,0)** | | (1,5) | (6,1) | (14,6) | (24,5) | (31,1) | (32,7) | (34,5) | (36,4) | (38,2) | (40,1) | (40,8) | (39,9) | (38,6) | - |
| Public Cloud PSN Managed (rivendita CSP) | **(195,5)** | | - | - | - | (1,9) | (4,9) | (10,0) | (17,6) | (24,2) | (28,2) | (33,5) | (33,9) | (27,0) | (14,4) | - |
| PaaS Industry (quota soci) | **(22,0)** | | - | (4,1) | (1,4) | (1,4) | (4,2) | (1,4) | (1,4) | (4,2) | (1,4) | (1,3) | (1,3) | - | - | - |
| PaaS Industry (quota PSN) | **(16,7)** | | - | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,6) | - | - | - |
| Hybrid Cloud on PSN Site | **(34,6)** | | - | (0,4) | (0,3) | (0,6) | (1,1) | (1,9) | (3,1) | (4,1) | (4,8) | (5,6) | (5,6) | (4,6) | (2,6) | - |
| Hybrid Cloud on PSN site (Quota CSP) | **(39,9)** | | - | - | - | (0,4) | (1,0) | (2,0) | (3,6) | (4,9) | (5,8) | (6,8) | (6,9) | (5,5) | (2,9) | - |
| Servizi di intra-migrazione | **(19,2)** | | - | - | - | (0,2) | (0,4) | (0,9) | (1,7) | (2,3) | (2,7) | (3,3) | (3,4) | (2,8) | (1,5) | - |
| Costi aggiuntivi | **(2,0)** | | - | (2,0) | - | - | - | - | - | - | - | - | - | - | - | - |
| Costi da migrazione | **(125,6)** | | (12,2) | (27,9) | (28,5) | (57,0) | - | - | - | - | - | - | - | - | - | - |
| Back-up | **(11,2)** | | (0,1) | (0,2) | (0,5) | (0,9) | (1,1) | (1,1) | (1,1) | (1,1) | (1,1) | (1,2) | (1,1) | (0,9) | (0,7) | - |
| **Costi indiretti** | **(143,1)** | | **(1,4)** | **(3,6)** | **(7,4)** | **(10,7)** | **(12,7)** | **(13,2)** | **(13,5)** | **(13,9)** | **(14,5)** | **(14,9)** | **(14,8)** | **(12,7)** | **(9,8)** | - |
| G&A - IT | **(95,9)** | | (0,5) | (1,9) | (4,4) | (6,9) | (8,6) | (9,0) | (9,2) | (9,6) | (10,0) | (10,4) | (10,2) | (8,7) | (6,6) | - |
| G&A - Altro | **(29,8)** | | (0,5) | (1,0) | (2,0) | (2,3) | (2,6) | (2,7) | (2,7) | (2,8) | (2,9) | (2,9) | (2,9) | (2,5) | (2,0) | - |
| Personale Staff | **(17,4)** | | (0,4) | (0,7) | (1,0) | (1,5) | (1,5) | (1,5) | (1,6) | (1,6) | (1,6) | (1,6) | (1,6) | (1,5) | (1,2) | - |
| **Costi straordinari** | - | | | | | | | | | | | | | | | |
| Contingency | - | | | | | | | | | | | | | | | |
| **Totale Costi Operativi** | **(2.436,8)** | | **(49,7)** | **(122,3)** | **(161,7)** | **(245,2)** | **(212,9)** | **(228,4)** | **(189,3)** | **(207,8)** | **(217,1)** | **(231,1)** | **(228,5)** | **(194,5)** | **(148,3)** | - |
| | - | | | | | | | | | | | | | | | |
| **Margine Operativo Lordo** | **632,71** | | **(6,5)** | **(2,7)** | **11,2** | **29,3** | **40,0** | **45,8** | **60,0** | **66,3** | **77,9** | **87,9** | **90,6** | **76,4** | **56,4** | - |
| | | | **(0,3)** | **(0,1)** | **0,0** | **0,1** | **0,1** | **0,1** | **0,2** | **0,2** | **0,2** | **0,3** | **0,3** | **0,3** | **0,2** | **#DIV/0!** |

HERMES ASSEVERAZIONI SRL
Via Ermete Novelli, 17
40127 Bologna
P. IVA e C.F. 03548511207

**Tabella 2: Piano Economico Finanziario - Conto Economico**

| | Totale | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ammortamenti** | | | | | | | | | | | | | | | | |
| Ammortamento asset materiali | **(269,5)** | | (3,0) | (9,2) | (16,6) | (24,0) | (28,1) | (28,5) | (27,3) | (26,3) | (25,4) | (24,8) | (22,6) | (18,0) | (11,4) | (4,4) |
| Ammortamento asset immateriali | **(35,5)** | | (1,1) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (2,8) | (1,1) |
| Ammortamento diritti d'uso | **(69,7)** | | (2,7) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | (5,6) | - |
| Ammortamento opex capitalizzate | **(14,1)** | | - | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | (1,17) | - |
| **Totale ammortamenti** | **(388,8)** | | **(6,7)** | **(18,8)** | **(26,2)** | **(33,5)** | **(37,6)** | **(38,0)** | **(36,9)** | **(35,9)** | **(34,9)** | **(34,3)** | **(32,1)** | **(27,6)** | **(20,9)** | **(5,5)** |
| **Risultato Operativo** | **243,87** | | **(13,3)** | **(21,4)** | **(15,0)** | **(4,3)** | **2,4** | **7,8** | **23,2** | **30,4** | **43,0** | **53,6** | **58,4** | **48,9** | **35,5** | **(5,5)** |
| **Gestione finanziaria** | | | | | | | | | | | | | | | | |
| Proventi finanziari | | | | | | | | | | | | | | | | |
| Oneri finanziari - finanziamenti | **(76,7)** | | (3,1) | (5,0) | (6,0) | (6,7) | (7,9) | (7,9) | (7,9) | (7,6) | (7,3) | (6,3) | (4,8) | (3,2) | (2,3) | (0,6) |
| Oneri finanziari - Debiti da leasing | **(15,6)** | | (1,9) | (1,9) | (1,8) | (1,8) | (1,6) | (1,4) | (1,3) | (1,1) | (0,9) | (0,8) | (0,6) | (0,4) | (0,2) | (0,0) |
| **Totale gestione finanziaria** | **(92,3)** | | **(5,0)** | **(6,8)** | **(7,9)** | **(8,4)** | **(9,5)** | **(9,4)** | **(9,2)** | **(8,7)** | **(8,3)** | **(7,1)** | **(5,4)** | **(3,6)** | **(2,5)** | **(0,6)** |
| Proventi e oneri straordinari | **-** | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Risultato prima delle Imposte** | **151,56** | | **(18,2)** | **(28,3)** | **(22,8)** | **(12,7)** | **(7,1)** | **(1,5)** | **13,9** | **21,7** | **34,7** | **46,6** | **53,0** | **45,3** | **33,0** | **(6,1)** |
| Imposte sul reddito di esercizio | **(50,0)** | | - | - | - | - | (0,1) | (0,4) | (1,1) | (1,7) | (3,6) | (5,3) | (15,2) | (13,0) | (9,5) | - |
| **Utile (Perdita) d'esercizio** | **101,51** | | **(18,2)** | **(28,3)** | **(22,8)** | **(12,7)** | **(7,2)** | **(1,9)** | **12,8** | **20,0** | **31,1** | **41,3** | **37,8** | **32,3** | **23,5** | **(6,1)** |

ASSEVERAZIONI SRL
Via Ermete Novelli, 1
40127 Bologna
P. IVA 035.4851207

**Tabella 3: Piano Economico Finanziario - Conto Finanziario**

| | Totale | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Area Operativa** | | | | | | | | | | | | | | | | |
| **Ebitda Adjusted** | **547,4** | | (8,8) | (5,5) | 6,1 | 21,7 | 32,4 | 38,2 | 52,5 | 58,8 | 70,4 | 80,5 | 83,1 | 69,0 | 49,0 | - |
| **Variazioni capitale circolante netto operativ** | **(50,6)** | | (21,3) | (11,6) | (15,0) | (21,8) | 8,7 | (8,7) | 3,6 | (8,9) | (3,3) | (2,6) | 0,7 | 12,7 | 16,9 | 50,6 |
| **Variazioni linea IVA** | **34,1** | | 24,1 | 10,5 | 11,1 | 16,6 | (12,2) | 6,8 | (8,3) | 6,8 | (0,6) | (0,7) | (1,6) | (8,0) | (10,3) | (34,1) |
| **Tasse** | **(50,0)** | | - | - | - | - | (0,1) | (0,4) | (1,1) | (1,7) | (3,6) | (5,3) | (15,2) | (13,0) | (9,5) | - |
| **Free Cash Flow Operativo** | **480,96** | | **(6,0)** | **(6,6)** | **2,2** | **16,5** | **28,8** | **35,9** | **46,7** | **55,0** | **63,0** | **71,8** | **67,0** | **60,7** | **46,1** | **16,4** |
| **Funding/rilascio conto di riserva** | **0,0** | | - | - | - | (54,8) | (9,9) | 8,3 | 11,8 | 13,9 | 8,3 | - | - | 22,5 | - | - |
| **Investimenti** | | | | | | | | | | | | | | | | |
| Infrastruttura IT | **(216,4)** | | (25,7) | (27,3) | (40,0) | (28,2) | (2,7) | (19,4) | (20,3) | (28,8) | (20,0) | (3,3) | (0,3) | (0,3) | (0,3) | - |
| Sistemi di sicurezza | **(11,3)** | | (0,5) | (1,2) | (1,2) | (2,4) | (0,1) | (0,6) | (1,2) | (1,4) | (2,4) | (0,2) | - | - | - | - |
| PDL (Postazioni di Lavoro) | **(0,5)** | | (0,3) | (0,1) | (0,1) | - | - | (0,0) | - | (0,0) | - | - | - | - | - | - |
| Licenze software | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Connettività | **(3,0)** | | (1,5) | - | - | - | - | (1,5) | - | - | - | - | - | - | - | - |
| Spazi attrezzati | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| IT | **(8,2)** | | (1,9) | (0,1) | (0,3) | (0,5) | (0,6) | (0,6) | (0,6) | (0,6) | (0,7) | (0,7) | (0,7) | (0,6) | (0,4) | - |
| Hybrid Cloud on PSN Site | **(20,0)** | | - | - | - | (0,6) | (0,9) | (1,6) | (2,9) | (2,9) | (2,8) | (4,5) | (3,0) | (0,7) | - | - |
| Costi di progetto | **(28,1)** | | (28,1) | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PaaS Industry | **(11,8)** | | - | (4,0) | - | - | (4,0) | - | - | (3,9) | - | - | - | - | - | - |
| Altre Capex | **(14,1)** | | (14,1) | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Free Cash Flow Operativo Post Investiment** | **181,60** | | **(78,1)** | **(39,2)** | **(39,4)** | **(70,0)** | **10,6** | **20,5** | **33,5** | **31,2** | **45,3** | **63,1** | **63,0** | **81,6** | **45,4** | **16,4** |
| **Erogazioni debito** | | | | | | | | | | | | | | | | |
| Accensione nuovi finanziamenti | **171,4** | | 59,6 | 29,7 | 30,6 | 51,5 | - | - | - | - | - | - | - | - | - | - |
| **Erogazione equity** | | | | | | | | | | | | | | | | |
| Apporto degli azionisti | **105,2** | | 29,0 | 28,3 | 22,8 | 25,1 | - | - | - | 0,0 | - | - | - | - | - | - |
| **Servizio del debito** | | | | | | | | | | | | | | | | |
| Rimborso nuovi prestiti a medio-lungo termine | **(171,4)** | | - | - | - | - | (2,2) | (9,3) | (16,5) | (18,2) | (28,4) | (38,8) | (40,1) | (17,9) | - | - |
| Interessi Capex | **(46,7)** | | (2,1) | (3,4) | (4,2) | (4,5) | (5,4) | (5,5) | (5,4) | (5,1) | (4,6) | (3,6) | (2,2) | (0,7) | - | - |
| Interessi linea IVA | **(29,4)** | | (1,0) | (1,6) | (1,9) | (2,2) | (2,5) | (2,4) | (2,5) | (2,5) | (2,7) | (2,7) | (2,7) | (2,5) | (2,3) | (0,6) |
| Financing fees | **(7,5)** | | (7,5) | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Servizio del debito** | **(255,0)** | | **(10,5)** | **(5,0)** | **(6,0)** | **(6,7)** | **(10,1)** | **(17,2)** | **(24,4)** | **(25,8)** | **(35,7)** | **(45,1)** | **(45,0)** | **(21,1)** | **(2,3)** | **(0,6)** |
| Cassa minima | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Free Cash Flow to Equity** | **203,31** | | **-** | **13,8** | **7,9** | **(0,0)** | **0,5** | **3,3** | **9,1** | **5,4** | **9,6** | **18,0** | **18,0** | **60,5** | **43,1** | **15,8** |
| **Dividendi** | **(189,2)** | | - | - | - | - | (13,0) | - | (10,9) | (16,0) | (9,6) | (18,0) | (18,0) | (60,5) | (43,1) | (15,8) |
| **Distribuzione Utili Portati a Nuovo** | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Variazione posizione finanziaria a breve** | **14,09** | | **-** | **13,8** | **7,9** | **(0,0)** | **(12,5)** | **3,3** | **(1,8)** | **(10,7)** | **0,0** | **(0,0)** | **(0,0)** | **(0,0)** | **0,0** | - |

RILIEVES ASSEVERAZIONI SRL
Via Ermete Novelli, 1
41127 Bologna
P. IVA C.F. 03455551207

## Tabella 4: Piano Economico Finanziario - Stato Patrimoniale

| | Anno -1 | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Attivo** | | | | | | | | | | | | | | | |
| **Crediti verso i soci per versamenti ancora dovuti (A)** | | | | | | | | | | | | | | | |
| Immobilizzazioni immateriali lorde | | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 | 49,6 |
| Fondo ammortamento immobilizzazioni immateriali | | (1,1) | (5,0) | (9,0) | (12,9) | (16,9) | (20,9) | (24,8) | (28,8) | (32,7) | (36,7) | (40,6) | (44,6) | (48,5) | (49,6) |
| **Immobilizzazioni immateriali nette** | | **48,5** | **44,6** | **40,6** | **36,7** | **32,7** | **28,8** | **24,8** | **20,9** | **16,9** | **12,9** | **9,0** | **5,0** | **1,1** | **-** |
| Immobilizzazioni materiali lorde | | 30,0 | 62,6 | 104,2 | 135,8 | 144,1 | 167,8 | 192,8 | 230,4 | 256,3 | 265,0 | 269,0 | 270,6 | 271,3 | 271,3 |
| Fondo ammortamento immobilizzazioni materiali | | (3,0) | (12,2) | (28,8) | (52,8) | (80,9) | (109,4) | (136,7) | (163,0) | (188,4) | (213,2) | (235,8) | (253,8) | (265,1) | (269,5) |
| **Immobilizzazioni materiali nette** | | **27,0** | **50,4** | **75,4** | **83,0** | **63,2** | **58,4** | **56,1** | **67,4** | **67,9** | **51,9** | **33,3** | **16,8** | **6,2** | **1,8** |
| Diritti d'uso immobili (data center) | | 67,0 | 61,4 | 55,8 | 50,3 | 44,7 | 39,1 | 33,5 | 27,9 | 22,3 | 16,8 | 11,2 | 5,6 | - | - |
| Immobilizzazioni finanziarie | | | | | | | | | | | | | | | |
| **Totale Immobilizzazioni (B)** | | **142,5** | **156,4** | **171,9** | **169,9** | **140,5** | **126,2** | **114,4** | **116,2** | **107,1** | **81,6** | **53,4** | **27,4** | **7,2** | **1,8** |
| Rimanenze | | | | | | | | | | | | | | | |
| Crediti commerciali | | 14,2 | 39,3 | 56,9 | 90,2 | 83,2 | 90,1 | 82,0 | 90,1 | 97,0 | 104,9 | 104,9 | 89,1 | 67,3 | - |
| Attività finanziarie non immobilizzazioni | | | | | | | | | | | | | | | |
| Cassa e Disponibilità liquide | | - | 13,8 | 21,7 | 21,7 | 9,2 | 12,5 | 10,7 | - | - | - | - | - | - | - |
| MRA + DSRA | | - | - | - | 54,8 | 64,7 | 56,5 | 44,7 | 30,8 | 22,5 | 22,5 | 22,5 | - | - | - |
| Crediti tributari | | 24,1 | 34,6 | 45,6 | 62,2 | 50,0 | 56,8 | 48,5 | 55,3 | 54,8 | 54,0 | 52,4 | 44,4 | 34,1 | - |
| **Totale Attivo circolante (C)** | | **38,3** | **87,7** | **124,2** | **229,0** | **207,1** | **215,9** | **185,8** | **176,2** | **174,3** | **181,5** | **179,9** | **133,5** | **101,4** | **-** |
| **Ratei e Risconti (D)** | | | | | | | | | | | | | | | |
| **Totale Attivo (A+B+C+D)** | | **180,8** | **244,1** | **296,1** | **398,9** | **347,6** | **342,1** | **300,2** | **292,4** | **281,4** | **263,0** | **233,3** | **160,9** | **108,7** | **1,8** |
| **Passivo** | | | | | | | | | | | | | | | |
| Capitale sociale | | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 |
| Riserva veramento soci | | 26,0 | 54,3 | 77,1 | 102,2 | 89,2 | 89,2 | 78,3 | 62,3 | 52,7 | 48,2 | 48,2 | 39,6 | 20,0 | 4,3 |
| Riserva Legale | | - | - | - | - | - | - | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 |
| Utili (perdite) portati a nuovo | | (18,2) | (46,5) | (69,3) | (82,0) | (89,2) | (91,1) | (78,9) | (58,9) | (27,8) | - | 19,8 | - | - | (6,1) |
| **Totale Patrimonio Netto (A)** | | **10,8** | **10,8** | **10,8** | **23,2** | **3,0** | **1,1** | **3,0** | **7,0** | **28,5** | **51,8** | **71,5** | **43,2** | **23,6** | **1,8** |
| **Fondi per rischi e Oneri (B)** | | | | | | | | | | | | | | | |
| **Trattamento di fine rapporto di lavoro subordinato (C)** | | | | | | | | | | | | | | | |
| Debiti commerciali | | 16,9 | 40,9 | 54,5 | 82,6 | 72,0 | 77,1 | 64,2 | 70,3 | 73,3 | 77,9 | 77,0 | 65,9 | 50,8 | - |
| Linea IVA | | 24,1 | 34,6 | 45,6 | 62,2 | 50,0 | 56,8 | 48,5 | 55,3 | 54,8 | 54,0 | 52,4 | 44,4 | 34,1 | - |
| Debiti finanziari a breve termine | | | | | | | | | | | | | | | |
| Debiti finanziari a lungo termine | | 59,6 | 89,3 | 119,9 | 171,4 | 169,2 | 159,9 | 143,5 | 125,3 | 96,8 | 58,1 | 17,9 | - | - | - |
| Debiti per leasing (data center) | | 69,3 | 68,4 | 65,1 | 59,3 | 53,3 | 47,2 | 40,9 | 34,5 | 27,9 | 21,1 | 14,3 | 7,2 | 0,0 | 0,0 |
| Altri Debiti | | 0,0 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | - |
| **Totale debiti (D)** | | **170,0** | **233,3** | **285,3** | **375,7** | **344,6** | **341,1** | **297,2** | **285,4** | **252,9** | **211,3** | **161,8** | **117,7** | **85,0** | **0,0** |
| **Ratei e Risconti (E)** | | | | | | | | | | | | | | | |
| **Totale Passivo (A+B+C+D+E)** | | **180,8** | **244,1** | **296,1** | **398,9** | **347,6** | **342,1** | **300,2** | **292,4** | **281,4** | **263,0** | **233,3** | **160,9** | **108,7** | **1,8** |

HERVE' ASSICURAZIONI SRL
Via Ermete Novelli, 1
40127 Bologna
P. IVA e C.F. 035.4851207

PSN
Polo strategico nazionale

# Polo Strategico Nazionale

## Relazione Illustrativa al Piano Economico Finanziario

Agosto 2022

INDICE DEI CONTENUTI

I. Premessa ..... 1
II. I Servizi Offerti dal PSN alle Pubbliche Amministrazioni (PA) ..... 4
III. Durata della Concessione, Adesione e Tempi di Migrazione ..... 7
IV. Investimenti e Ammortamento Finanziario ..... 8
V. Costi Operativi ..... 10
VI. Operating Leases ..... 15
VII. Tariffe e Ricavi ..... 16
VIII. Ipotesi macroeconomiche, fiscali e capitale circolante ..... 19
IX. Ipotesi Finanziarie ..... 20
X. Indicatori dell'Equilibrio Economico-Finanziario ..... 22
XI. Analisi dei Rischi ..... 23

# I. Premessa

1. Il Piano Triennale per l'informatica nella pubblica amministrazione (PA), approvato con DPCM del 31 maggio 2017, ha avviato un percorso di razionalizzazione e riqualificazione delle infrastrutture ICT[1] della PA italiana improntato sul principio tecnologico del "Cloud first", che consentirà alle PA di offrire un utilizzo più efficiente e flessibile delle risorse ICT, con livelli elevati di economicità, affidabilità e sicurezza, e capace di favorire un'offerta di servizi sempre più adeguati alle esigenze di cittadini e imprese.

2. In linea con le prescrizioni del Piano Triennale, l'Agenzia per l'Italia Digitale (AgID)[2] ha effettuato un censimento del patrimonio ICT della PA, volto a classificare le infrastrutture ICT della PA in termini di affidabilità e sicurezza. Tale censimento si proponeva in particolare di individuare: (i) infrastrutture candidabili ad essere utilizzate dal Polo Strategico Nazionale (PSN), ossia l'insieme delle infrastrutture ad alta disponibilità qualificate ad erogare servizi IT ad altre PA in maniera continuativa e sistematica; (ii) infrastrutture non candidabili come PSN, ma con requisiti minimi di affidabilità e sicurezza (data center di tipo A), e (iii) e infrastrutture caratterizzate da carenze strutturali e organizzative o comunque non in grado di garantire affidabilità, sicurezza e continuità dei servizi (data center di tipo B).

3. Dal censimento, i cui risultati sono stati pubblicati da AgID con la delibera n. 1 del 14 giugno 2019, è emerso un quadro di elevata frammentazione, con livelli di sicurezza inadeguati ed elevata inefficienza in termini di spesa. Molti data center sono risultati energeticamente inefficienti, obsoleti, non sicuri e dispendiosi. Con riferimento specifico alle infrastrutture ICT delle pubbliche amministrazioni centrali (PAC), il censimento ha individuato 89 data center di tipo B, tutti caratterizzati da gravi carenze strutturali e organizzative.

4. Al fine di promuovere "lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e consolidamento dei centri per l'elaborazione delle informazioni", il DL Semplificazioni, convertito in legge l'11 settembre 2020, e recante "misure urgenti per la semplificazione e l'innovazione digitale", ha previsto che le PAC dotate di data center di tipo B, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, abbiano l'obbligo di migrare i loro centri per l'elaborazione delle informazioni e i relativi sistemi informatici verso strutture idonee, da individuare tra (i) il costituendo PSN, (ii) infrastrutture già esistenti e in possesso dei requisiti, (iii) l'infrastruttura della Società Generale d'Informatica (Sogei), qualora venisse resa compatibile con i requisiti del regolamento AgID, o alternativamente (iv) soluzioni di public cloud per i servizi non critici.

---

[1] Information and Communications Technology.

[2] AgID è l'agenzia tecnica della Presidenza del Consiglio dei Ministri (PCM) con il compito di garantire la realizzazione degli obiettivi dell'Agenda Digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie ICT. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese.

5. Le misure del DL Semplificazione si inseriscono in un piano complessivo di trasformazione dell'IT della PA promosso dal Governo, che pone la componente infrastrutturale al centro, con l'obiettivo di realizzare un modello Cloud della PA improntato al principio del "Cloud First" per facilitare la migrazione dei servizi, promuovere la razionalizzazione e il consolidamento dei data center, e ottenere maggiore efficacia ed efficienza. Il PSN avrà un ruolo centrale all'interno di questo piano, in quanto sarà il soggetto titolare di quell'insieme di infrastrutture IT qualificato ad erogare servizi ICT alle altre PA.

6. In un contesto di mercato del cloud attualmente caratterizzato dalla presenza di colossi stranieri, Cassa Depositi e Prestiti S.p.A. attraverso la sua controllata CDP Equity S.p.A. (CDPE), Leonardo S.p.A. (Leonardo). Società Generale d'Informatica S.p.A. (Sogei), e Telecom Italia S.p.A. (TIM) si sono fatte promotrici del progetto di realizzazione del PSN per le PAC (Progetto).

7. Il 28 gennaio 2022 è stato pubblicato il bando per la realizzazione del Polo Strategico Nazionale (PSN). La proposta per la creazione del Polo, su cui si basa la gara, è stata individuata dal Dipartimento a dicembre 2021 secondo il modello di partenariato pubblico privato. La procedura è affidata a Difesa Servizi S.p.A., società in house del Ministero della Difesa, in qualità di centrale di committenza. Il raggruppamento composto da CDP Equity, Leonardo, Sogei e TIM partecipano alla gara in qualità di soggetto promotore, avendo presentato una proposta spontanea a dicembre 2021 che è stata dichiarata di pubblico interesse e che è stata posta a base di gara.

8. Il 22 giugno 2022 è risultata aggiudicataria del bando di gara di cui al punto precedente la cordata composta da Fastweb e Aruba, lasciando al raggruppamento una finestra temporale di 15 giorni per valutare la possibilità di esercitare il diritto di prelazione in qualità di promotore. Tale diritto è stato esercitato entro i termini previsti, motivo per cui il raggruppamento composto da CDP Equity, Leonardo, Sogei e TIM è risultato in via definitiva l'aggiudicatario del bando di gara.

9. CDP Equity, Leonardo, Sogei e TIM rappresentano una compagine industriale nazionale in grado di offrire una soluzione cloud alle PAC di altissima qualità:

    a. TIM è una delle maggiori società di telecomunicazioni al mondo, e leader in Italia per innovazione tecnologica infrastrutturale e servizi di Cloud e connettività per le PA,

    b. CDP Equity, società di investimento controllata al 100% dal gruppo CDP, a sua volta controllata dal Ministero dell'economia e delle finanze, è il principale soggetto attuatore della politica industriale italiana attraverso investimenti in settori strategici quali le infrastrutture di rilevanza critica.

    c. Leonardo è una delle maggiori realtà industriali internazionali operanti nei settori aerospaziale, della difesa e della sicurezza con una importante Divisione Cyber & Security Solutions specializzata nel settore della sicurezza e trasformazione digitale.

    d. Sogei, società d'informatica interamente controllata dal Ministero dell'Economia e delle Finanze, è la "piattaforma digitale" dell'Amministrazione Finanziaria italiana e costituisce una risorsa unica per il Paese in termini di efficienza, solidità, sicurezza e alta affidabilità, capace di tradurre le esigenze di innovazione in benefici per cittadini, imprese e istituzioni.

10. Il Progetto presentato da TIM, CDPE, Leonardo e Sogei prevede la costituzione di una società di servizi a cui venga affidata in concessione, tramite gara e in project financing, la realizzazione e gestione del Polo Strategico Nazionale (PSN).

11. Il PSN offrirà i propri servizi a tutte le PA interessate, incluse le PAC con data center di tipo B e le PA locali, e alle Aziende Sanitarie Locali (ASL) che vi vorranno aderire. Il Progetto prevede la costituzione di quattro data center, due nel Lazio e due in Lombardia, capaci di offrire servizi ICT alle PA e alle ASL che decideranno di migrare i loro data center al PSN.

12. Il PSN offrirà ai soggetti aderenti (le "Amministrazioni utenti" o "Amministrazioni") (i) servizi infrastrutturali *on-demand*, (ii) servizi di *disaster recovery* e *business continuity*, (iii) servizi di gestione della sicurezza, e (iv) servizi di assistenza. Le PAC avranno un periodo di 36 mesi dall'assegnazione della concessione per decidere se aderire al PSN, salvo proroga concordata fra Concedente e Concessionario che prolungherebbe il periodo di migrazione a 48 mesi, e aderiranno al servizio tramite il pagamento dei prezzi di listino, al netto dello sconto offerto, per i servizi erogati.

13. La presente relazione illustra i principali presupposti operativi, economici e finanziari del Piano Economico Finanziario (PEF) relativo all'iniziativa in questione.

14. In particolare:

    a. La sezione II descrive i servizi offerti dal PSN alle Amministrazioni utenti;

    b. La sezione III descrive la durata della concessione e le assunzioni operative del PEF relativamente al numero di Amministrazioni utenti che aderiranno al servizio e ai tempi necessari per portare a termine la migrazione dei servizi;

    c. La sezione IV descrive il piano degli investimenti e le assunzioni relative all'ammortamento finanziario.;

    d. La sezione V descrive l'andamento dei costi operativi monetari, esclusi i canoni di locazione degli spazi attrezzati;

    e. La sezione VI descrive il trattamento dei canoni di locazione degli spazi attrezzati all'interno dei data center, che sono capitalizzati nello stato patrimoniale come *operating lease liabilities* secondo i principi contabili di IFRS 16;

    f. La sezione VI descrive l'andamento di tariffe e ricavi;

    g. Le sezioni VIII e IX descrivono le assunzioni macroeconomiche utilizzate per le previsioni, le ipotesi finanziarie relative al finanziamento del progetto e le assunzioni fiscali;

    h. La sezione X presenta gli indici relativi all'equilibrio economico-finanziario del progetto;

    i. La sezione XI, infine, riporta la matrice dei rischi con la ripartizione dei rischi dei tra Concedente e Concessionario.

# II. I Servizi Offerti dal PSN alle Pubbliche Amministrazioni (PA)

15. Il PSN offrirà:

    a. Servizi infrastrutturali on-demand di tipo tradizionale, private cloud;

    b. Servizi di gestione della sicurezza IT;

    c. Servizi di *disaster recovery* e *business continuity*;

    d. Servizi Professionali a supporto delle amministrazioni;

    e. Servizi di assistenza ai fruitori dei servizi erogati.

16. I principali servizi infrastrutturali on-demand sono rappresentati dai servizi di Housing, Hosting, Infrastructure as a Service (IaaS) e Cloud, cui si aggiungono una varietà di servizi complementari.

    a. **Housing**: I servizi di Housing prevedono l'utilizzo di uno spazio fisico dedicato all'interno dei data center del PSN. Il PSN si occuperà dell'attivazione iniziale e della gestione base degli spazi attrezzati. I server rimarranno di proprietà della Amministrazione interessata, che si occuperà della gestione operativa dei servizi senza vincoli o contributi esterni.

    b. **Hosting**: I servizi di Hosting prevedono il noleggio di server dedicati all'interno dei data center del PSN. Il PSN si occuperà dell'allaccio e della gestione complessiva dei server. Il servizio verrà erogato in due modalità: (i) hosting dedicato su rack condivisi, per cui le Amministrazioni avranno accesso dedicato a porzioni di rack condivisi con altre PA, e (ii) hosting dedicato su rack privati.

    c. **IaaS Private** e **Iaas Shared**: i servizi di IaaS (Private e Shared) prevedono il noleggio di spazi fisici o virtuali, dedicati o non dedicati all'interno dei data center del PSN e l'utilizzo di un'infrastruttura IT altamente automatizzata e scalabile.

    d. **Altri servizi di IaaS e Cloud**: Congiuntamente ai servizi principali di IaaS (Private e Shared), il PSN offrirà alle Amministrazioni utenti altri servizi IaaS e Cloud specifici e/o complementari, e in particolare:

        i. **Platform as a Service (PaaS)**: I servizi PaaS sono servizi di cloud computing e prevedono che il PSN metta a disposizione delle Amministrazioni utenti una piattaforma virtuale per sviluppare e gestire applicazioni per offrire i propri servizi senza la necessità di costruire e mantenere l'infrastruttura necessaria. Comprende inoltre i seguenti servizi PaaS Industry: DBaaS, PaaS IAM, Big Data e AI, piattaforme in grado di erogare elementi applicativi e middleware come servizio (database, big data, AI).

        ii. **Containers-as-a-Service (CaaS)**: I servizi CaaS sono servizi di cloud computing analoghi ai PaaS, ma prevedono che il PSN metta a disposizione delle Amministrazioni utenti dei container. Gli sviluppatori di software e i reparti IT potranno quindi caricare, organizzare, eseguire, scalare, gestire e arrestare i container. Il servizio CaaS si colloca a metà strada tra IaaS e PaaS.

iii. **Disaster Recovery as a Service (DRaaS)**: il PSN offrirà inoltre servizi di Disaster Recovery per le infrastrutture IaaS e Cloud.

e. **Sistemi operativi**: è il servizio di fornitura dei sistemi operativi utilizzati per i servizi IaaS.

f. **Hybrid Cloud on PSN Site**: il PSN offrirà servizi del Public Cloud Provider "perimetrati" (in termini di numero di utenti con accesso limitato e di servizi rispetto al servizio originale del Cloud provider) e installati sull'infrastruttura locale del PSN.

g. **Public Cloud PSN Managed**: il PSN offrirà un portfolio dei servizi «Hyperscaler» erogato da "Region" dedicata al PSN, con separazione logico/fisica e operata e controllata da personale PSN.

h. **Secure Public Cloud**: il PSN offrirà servizi di sicurezza a "valore aggiunto" integrati ai servizi base «Hyperscaler» tramite servizi professionali per la securizzazione.

i. **Migrazione**: il PSN offrirà servizi necessari a permettere la migrazione delle Amministrazioni utente sulle infrastrutture del PSN.

j. **Business & Culture Enablement**: il PSN offrirà servizi di consulenza alle Amministrazioni utenti per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità.

k. **Servizi professionali di sicurezza**: Servizi professionali specialistici per il miglioramento della sicurezza delle infrastrutture e delle applicazioni della PA

l. **Replatform e Rearchitect**: il PSN offrirà servizi professionali evolutivi volti al ridisegno delle applicazioni in ottica Cloud.

m. **IT infrastructure - service operations**: il PSN offrirà servizi professionali a supporto delle Operations dell'infrastruttura e del parco applicativo cliente.

17. All'interno del PEF, l'insieme dei servizi di Housing, Hosting, IaaS, altri servizi, Hybrid Cloud on PSN Site e Public Cloud PSN Managed, Secure Public Cloud e migrazione costituisco i **Servizi Core**.

18. Il PSN offrirà i propri servizi consentendo alle Amministrazioni utenti di selezionare il tipo di servizio più idoneo per erogare i propri servizi a cittadini e imprese, con diversi livelli di integrazione nel cloud, e adottando anche un modello di hybrid cloud con flessibilità tecnologica.

19. La Tabella 1 sintetizza gli elementi dell'offerta del PSN alle Amministrazioni per tipologia di servizio infrastrutturale.

## TABELLA 1: SERVIZI EROGATI DAL PSN

| Elementi di offerta | Housing | Hosting | IaaS | Cloud |
|---|---|---|---|---|
| Connettività, Rack e cablaggi | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Connettività, LAN | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Connettività, WAN | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Connettività, Rete Geografica (da PAC a PSN) | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Spazio attrezzato | ✓ Incluso nell'offerta | ✓ Incluso nell'offerta | ✓ Incluso nell'offerta | ✓ Incluso nell'offerta |
| Energia | ✓ Inclusa nell'offerta (3 KW/rack) | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Sicurezza | ✓ Fisica, DR, Endpoint e NTW security | ✓ + Id. & access, key mgmt, cyber gov. | ✓ + cyber monit., vulner. & testing mgmt | ✓ Inclusa nell'offerta |
| Hardware, rack | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta |
| Hardware, server dedicati | ✗ - | ✓ Inclusi nell'offerta, tutti | ✓ Inclusi nell'offerta | ✗ - |
| Hardware, server condivisi | ✗ - | ✗ - | ✗ - | ✓ Inclusi nell'offerta |
| Hardware, storage (Flash e SATA) | ✗ - | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta |
| SW (OS, Virtualiz., Hypervisor), no gestione | ✗ - | ✓ Inclusi nell'offerta (SO) | ✓ Inclusi nell'offerta | ✓ Inclusi nell'offerta |
| SW, Gestione | ✗ - | ✗ - | ✓ Inclusa nell'offerta | ✓ Inclusa nell'offerta |
| Accesso a capacità computaz. on demand | ✗ - | ✗ - | ✓ Flat (non a consumo): 24/7/365 anno | ✓ Flat (non a consumo): 24/7/365 anno |
| Servizi di Migrazione infrastrutturale | ✓ Inclusi nell'offerta, da quotare on top | ✓ Inclusi nell'offerta, da quotare on top | ✓ Inclusi nell'offerta, da quotare on top | ✓ Inclusi nell'offerta, da quotare on top |

# III. Durata della Concessione, Adesione e Tempi di Migrazione

20. **Durata della Concessione:** Il PEF è stato redatto ipotizzando che la concessione abbia una durata di 13 anni dall'assegnazione. All'avvio del progetto, il PEF prevede una fase iniziale di progettazione e allestimento di tre anni, durante la quale le Amministrazioni aderenti dovranno migrare i propri servizi. La fornitura dei servizi avrà poi una durata di 120 mesi (10 anni) decorrenti dalla data di adesione di ciascuna Amministrazione. Le Amministrazioni avranno 36 mesi dall'assegnazione della concessione per decidere se aderire al progetto e potranno effettivamente migrare i propri servizi entro i 48 mesi successivi all'avvio del progetto. Qualora la percentuale di migrazione sia inferiore rispetto a quella prevista dal PEF, i periodi di migrazione e di adesione saranno automaticamente estesi di ulteriori 18 mesi. La durata della concessione è coerente con l'orizzonte temporale necessario all'ammortamento integrale degli investimenti ed al raggiungimento dell'equilibrio economico-finanziario.

21. **Adesioni e tempi di migrazione:** Il PEF prevede una percentuale di adesione pari al 70% per le PAC con data center di tipo B, al 50% per le ASL, e all'1% per le altre PA locali. Il PEF prevede che tutte le Amministrazioni aderenti migreranno i propri data center nell'arco di 48 mesi dall'avvio del progetto. Delle Amministrazioni che aderiscono, Il PEF prevede una migrazione del 10% nel primo anno, che sale al 33% nel secondo anno, il 55% nel terzo anno fino a raggiungere il 100% nel quarto anno.

# IV. Investimenti e Ammortamento Finanziario

22. **Investimenti:** Il PEF prevede investimenti per infrastruttura IT, sistemi di sicurezza, postazioni di lavoro, software, spazi attrezzati, IT, e costi di progettazione.

    a. **Infrastrutture IT**: gli investimenti per l'infrastruttura IT, complessivamente pari a € 216,4 milioni durante la durata della concessione, sono la principale voce degli investimenti e rappresentano il costo per la progettazione e la realizzazione delle infrastrutture IT necessarie allo svolgimento dei servizi offerti dal PSN. Il PEF calcola il valore degli investimenti in infrastrutture IT a partire da costi unitari delle apparecchiature (rack, enclosure, server, server blade, TB SATA, TB flash).

    b. **Sistemi di sicurezza**: gli investimenti per i sistemi di sicurezza sono complessivamente pari a € 11,3 milioni durante la durata della concessione, e rappresentano gli investimenti necessari ad implementare i sistemi di sicurezza software e hardware del PSN.

    c. **Postazioni di Lavoro**: gli investimenti per le postazioni di lavoro sono complessivamente pari a € 0,5 milioni durante la durata della concessione. Tali investimenti rappresentano i costi capitalizzati necessari a progettare e realizzare le postazioni di lavoro del PSN e sono stimati sulla base di un costo unitario di € 7 migliaia.

    d. **Connettività**: gli investimenti per la connettività sono complessivamente pari a € 3,0 milioni e rappresentano gli investimenti per predisporre la rete di connettività fra i data center del PSN. Vengono ipotizzati 4 data center per i quali i costi di connettività unitari sono pari ad € 350 migliaia.

    e. **IT**: gli investimenti per IT sono complessivamente pari a € 55,3 milioni, e rappresentano i gli investimenti necessari a allestire i sistemi hardware e software del PSN.

    f. **Hybrid Cloud on PSN Site:** gli investimenti per Hybrid Cloud on PSN site sono complessivamente pari a € 20,0 milioni e rappresentano gli investimenti necessari a allestire l'infrastruttura locale del PSN ad un prezzo unitario di € 28 migliaia per il numero di server necessari per soddisfare la domanda prevista.

    g. **Costi di progetto:** gli investimenti per costi di progetto sono complessivamente pari a € 28,1 milioni e rappresentano gli investimenti relativi ai servizi di consulenza necessari alla predisposizione del progetto.

    h. **PaaS Industry:** gli investimenti per PaaS Industry sono complessivamente pari a € 11,8 milioni e rappresentano gli investimenti necessari a mettere a disposizione le piattaforme in grado di erogare elementi applicativi e middleware come servizio (database, big data, AI).

    i. **Altre Capex:** gli investimenti per altre capex sono complessivamente pari a € 14,1 milioni e rappresentano dei costi di setup infrastrutturale da sostenere nel primo anno di attività.

23. **Evoluzione temporale degli investimenti:** La Tabella 2 mostra l'evoluzione degli investimenti nel corso della concessione. Il PEF prevede due cicli di investimenti, al primo e sesto anno di concessione, in quanto gli investimenti in infrastrutture IT hanno una vita utile pari a 5 anni.

**TABELLA 2: EVOLUZIONE DEGLI INVESTIMENTI DURANTE LA CONCESSIONE**

| Investimenti (€ mln) | Totale | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infrastruttura IT | **(216,4)** | (25,7) | (27,3) | (40,0) | (28,2) | (2,7) | (19,4) | (20,3) | (28,8) | (20,0) | (3,3) | (0,3) | (0,3) | (0,3) | - |
| Sistemi di sicurezza | **(11,3)** | (0,5) | (1,2) | (1,2) | (2,4) | (0,1) | (0,6) | (1,2) | (1,4) | (2,4) | (0,2) | - | - | - | - |
| PDL (Postazioni di Lavoro) | **(0,5)** | (0,3) | (0,1) | (0,1) | - | - | (0,0) | - | (0,0) | - | - | - | - | - | - |
| Licenze software | **-** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Connettività | **(3,0)** | (1,5) | - | - | - | - | (1,5) | - | - | - | - | - | - | - | - |
| Spazi attrezzati | **-** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| IT | **(8,2)** | (1,9) | (0,1) | (0,3) | (0,5) | (0,6) | (0,6) | (0,6) | (0,6) | (0,7) | (0,7) | (0,7) | (0,6) | (0,4) | - |
| Hybrid Cloud on PSN Site | **(20,0)** | - | - | - | (0,6) | (0,9) | (1,6) | (2,9) | (2,9) | (2,8) | (4,5) | (3,0) | (0,7) | - | - |
| Costi di progetto | **(28,1)** | (28,1) | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PaaS Industry | **(11,8)** | - | (4,0) | - | - | (4,0) | - | - | (3,9) | - | - | - | - | - | - |
| Altre Capex | **(14,1)** | (14,1) | - | - | - | - | - | - | - | - | - | - | - | - | - |

Fonte: PEF, Conto Finanziario.

24. **Ammortamenti:** Il PEF prevede un ammortamento tecnico sulla base della vita utile dei singoli investimenti, in particolare:

    a. Gli investimenti per le infrastrutture IT, sistemi di sicurezza, connettività, spazi attrezzati, PaaS Industry e IT hanno una vita utile pari a 5 anni.

    b. Gli investimenti per le postazioni di lavoro hanno una vita utile pari a 10 anni.

    c. Gli investimenti per le licenze software e per Hybrid Cloud on PSN Site hanno una vita utile pari a 3 anni.

    d. Gli investimenti relativi ai costi di progetto vengono ammortizzati lungo il corso dell'intera concessione, con una vita utile pari a 13 anni.

25. **Valore residuo:** Al termine del periodo di concessione il PEF prevede un valore residuo delle immobilizzazioni materiali pari a € 1,8 milioni. Tale valore rappresenta una stima dell'indennizzo di subentro che verrà pagato al concessionario uscente.

# V. Costi Operativi

26. Il PEF suddivide i costi operativi del PSN in costi di connettività, spazi attrezzati, energia, sicurezza, manutenzioni hardware, canoni software, ops tecniche (interne ed esterne), security operations, sicurezza CERT, controllo produzione IT, COPS, service management, IT infrastructure - service operations, servizi professionali di sicurezza, secure public cloud (suddividendo quota PSN e rivendita CSP), rearchitect, replatform, Business & Culture Enablement, public cloud PSN managed (suddividendo quota PSN e rivendita CSP), PaaS Industry (suddividendo quota PSN e quota soci), hybrid cloud on PSN site, servizi di intra-migrazione, back-up, G&A, personale staff e costi da migrazione. Di seguito si riportano le linee di costo che sono state identificate nella costruzione del PEF con i principali driver che guidano la loro evoluzione. Per un maggiore dettaglio circa le assunzioni si rimanda al foglio Controllo del PEF in formato xls.

    a. **Connettività**: i costi per servizi di connettività ammontano complessivamente a € 65,9 milioni. Tali costi rappresentano i servizi di connessione all'interno delle regioni Lazio-Lombardia e tra le due regioni, oltre che per il servizio DDOS. I costi aumentano negli anni della concessione sulla base dei volumi dei servizi IaaS, Cloud, PaaS e CaaS. Questi costi sono relativi a servizi forniti dai soci

    b. **Spazi attrezzati (esclusi i canoni d'affitto)**: i costi per gli spazi attrezzati, esclusi i canoni annuali per l'affitto degli spazi attrezzati all'interno dei data center, ammontano complessivamente a € 55,0 milioni. Tali costi rappresentano i costi operativi relativi agli spazi fisici necessari per ospitare l'infrastruttura ed evolvono in base al numero di metri quadri che si ipotizzano necessari per ospitare l'infrastruttura dedicata ed in base al prezzo al metro quadro stimato per ciascuna delle due sedi (Milano e Roma) e sulla base di un costo unitario dei rack di € 5.000 (oltre un canone una tantum di €3.500) al primo anno e che assumerà un andamento influenzato dai risparmi di costo attesi in funzione dell'evoluzione tecnologica e dall'incremento di costo relativo all'inflazione. Questi costi sono relativi a servizi forniti dai soci.

    c. **Energia**: i costi per l'energia ammontano complessivamente a € 105,1 milioni. Tali costi rappresentano i costi per l'energia utilizzata dal PSN e sono stati stimati ipotizzando un costo dell'energia nell'intorno di 0,23 €/KWh. Il prezzo unitario stimato riflette l'assunzione di normalizzazione dello scenario macroeconomico attuale, all'interno del quale i prezzi energetici sono estremamente volatili e sensibilmente superiori a quanto stimato ai fini del PEF (a titolo esemplificativo, alla data di redazione del presente documento i contratti future al 2023 erano quotati oltre 0,4 €/KWh), ai fini del quale sono stati ipotizzati dei valori più coerenti con le aspettative che questa situazione non si protrarrà in modo prolungato nel tempo. Questa componente potrà essere soggetta a scostamenti anche sensibili dalle stime effettuate in funzione di i) l'alta volatilità del sottostante e ii) la possibilità di effettuare operazioni di copertura bloccando i prezzi futuri limitatamente ai prossimi 2-3 anni, senza possibilità di effettuare copertura di più lunga durata. Questi costi sono sostenuti dai soci.

    d. **Sicurezza**: i costi di licenze SW per la sicurezza informatica ammontano complessivamente a € 47,1 milioni. Tali costi rappresentano i costi per (i) cybersecurity governance, (ii) cybersecurity monitoring, (iii) endpoint security, (iv) identity and access, (v) key management, (vi) network

security, e (vii) vulnerability & testing management. I costi evolvono nel corso della concessione sulla base del numero dei server in utilizzo che viene ipotizzato lungo la durata del PEF.

e. **Software**: i costi per software ammontano complessivamente a € 306,0 milioni. Tali costi rappresentano i costi relativi alle licenze per virtualizzatori/hypervisor (per i servizi IaaS, PaaS e CaaS), per sistemi operativi acquistati dalle amministrazioni e per le licenze software (servizi Paas), calcolati sulla base delle quantità di listino. Tali costi comprendono anche le spese per gli orchestrator, calcolati sulla base dei server virtuali e fisici e dei servizi che li utilizzano. Questi costi sono relativi a servizi forniti da terzi.

f. **Ops tecniche interne:** i costi per le ops interne ammontano complessivamente a € 32,1 milioni. Tali costi rappresentano i costi del personale tecnico interno del PSN. I costi evolvono nel corso della concessione sulla base del personale interno impiegato e del costo unitario per il personale interno (ipotizzato pari ad €56k/FTE), indicizzato all'inflazione. Questi costi sono legati al costo del personale interno.

g. **Ops tecniche esterne**: i costi per le ops esterne ammontano complessivamente a € 12,9 milioni. Tali costi rappresentano i costi per i servizi del PSN esternalizzati. I costi evolvono nel corso della concessione sulla base del personale esterno impiegato e del costo unitario per il personale esterno (ipotizzato pari ad €74k/FTE), indicizzato all'inflazione. Questi costi sono relativi a servizi forniti da terzi.

h. **Security Operations e Sicurezza CERT**: i costi per la security operations (SOC e CERT) ammontano complessivamente a € 103,4 milioni. Tali costi rappresentano i costi per i servizi di security del PSN e fanno riferimento a servizi offerti dai soci del PSN. I servizi evolvono sulla base del numero di rack in scope e del prezzo unitario per server che è stato ipotizzato.

i. **Controllo produzione IT**: i costi per il controllo della produzione IT ammontano complessivamente a € 96,9 milioni. Tali costi rappresentano i costi per i servizi di monitoraggio e gestione della produzione IT, supporto tecnico e prima manutenzione/intervento. Tali servizi sono offerti dai soci del PSN e sono parametrati al costo del personale interno e ai costi unitari previsti per ciascun servizio.

j. **COPS**: i COPS ammontano complessivamente a € 98,8 milioni. Tali costi rappresentano i costi di supporto tecnico alle Amministrazioni utenti. Tali servizi sono offerti dai soci del PSN e sono parametrati al costo del personale interno e ai costi unitari previsti per ciascun servizio.

k. **Service management**: i costi per service management ammontano complessivamente a € 21,0 milioni. Tali costi rappresentano i costi per servizi di gestione del cliente e monitoraggio dei servizi erogati del PSN. Tali servizi sono offerti dai soci del PSN e sono parametrati al costo del personale interno e ai costi unitari previsti per ciascun servizio.

l. **IT infrastructure - service operations**: i costi per IT infrastructure- service operations ammontano complessivamente a € 33,3 milioni. Tali costi sono parametrati ai costi per il personale che è stato previsto, differenziato per mansione, e alle ore di lavoro necessarie per ciascuna categoria. Questi costi sono relativi a servizi forniti dai soci.

m. **Servizi Professionali di Sicurezza**: i costi per i Servizi professionali di sicurezza ammontano complessivamente a € 77,9 milioni. Tali costi rappresentano i costi per i servizi di assessment, strategy & compliance, e supporto alle operations parametrati al numero di Amministrazioni aderenti al servizio e al costo del personale dedicato. Questi costi sono relativi a servizi forniti dai soci.

n. **Secure Public Cloud (quota PSN e rivendita CSP)**: i costi per Secure Public Cloud ammontano complessivamente a € 426,9 milioni. Tali costi rappresentano i costi per servizi di program governance, design, key management, template, back-up e erogazione del servizio, oltre ai costi riconosciuti agli hyperscaler per erogare i servizi. Questi sono parametrati al numero di Amministrazioni aderenti al servizio e al costo del personale. Questi costi sono relativi a servizi forniti in parte dai soci ed in parte da terzi.

o. **Rearchitect**: i costi per Rearchitect ammontano complessivamente a € 182,7 milioni. Tali costi sono parametrati al numero di Amministrazioni aderenti al servizio e al costo del personale. Questi costi sono relativi a servizi forniti dai soci.

p. **Replatform**: i costi per Replatform ammontano complessivamente a € 90,7 milioni. Tali costi sono parametrati al numero di Amministrazioni aderenti al servizio e al costo del personale. Questi costi sono relativi a servizi forniti dai soci.

q. **Business & Culture Enablement**: i costi per Business & Culture Enablement ammontano complessivamente a € 29,8 milioni. Tali costi rappresentano i costi relativi ai servizi di consulenza alle singole Amministrazioni, e sono parametrati alle PA che si stima usufruiranno del servizio e ai costi unitari assunti. Questi costi sono relativi a servizi forniti dai soci.

r. **Public Cloud PSN Managed (quota PSN e rivendita CSP)**: i costi per la Public Cloud PSN Managed ammontano complessivamente a € 236,8 milioni. Tali costi rappresentano i costi relativi alla fornitura di servizi "Hyperscaler" e sono parametrati al numero di server in scope. Questi costi sono relativi a servizi forniti in parte dai soci ed in parte da terzi.

s. **PaaS Industry (quota soci e quota PSN)**: i costi per PaaS Industry ammontano complessivamente a € 38,7 milioni. Tali costi rappresentano i costi relativi alla messa a disposizione di piattaforme in grado di erogare elementi applicativi e middleware come servizio (database, big data, AI). Si suddividono in costi relativi a hardware, software, spazi e manutenzione, parametrati al numero di Amministrazioni aderenti al servizio e al costo di approvvigionamento delle attrezzature. Questi costi sono relativi a servizi forniti in parte dai soci ed in parte da terzi.

t. **Hybrid Cloud on PSN Site**: i costi per Hybrid Cloud on PSN Site ammontano complessivamente a € 74,5 milioni. Tali costi rappresentano i costi necessari a offrire servizi del Public Cloud Provider "perimetrati" e installati sull'infrastruttura locale del PSN. Tali costi si riferiscono a costi di program governance, energia, connettività e spazi attrezzati, sicurezza infrastrutturale e design, parametrati al numero di Amministrazioni aderenti al servizio e al costo del personale. Questi costi sono relativi a servizi forniti in parte dai soci ed in parte da terzi.

u. **Servizio di migrazione e intra-migrazione**: Tali costi rappresentano i costi necessari a permettere la migrazione delle Amministrazioni nel PSN e della intra-migrazione tra servizi diversi

(permettendo un cambio mix infrastrutturale nel tempo verso servizi evolutivi). I costi evolvono sulla base dei costi di progettazione, analisi infrastrutturale, set up applicativo, set up infrastrutturale e supporto alla migrazione per i vari servizi offerti dal PSN. Tali servizi sono parametrati ai costi per il personale che è stato previsto, differenziato per mansione, e alle ore di lavoro necessarie per ciascuna categoria. Questi costi sono relativi a servizi forniti dai soci e valgono 125,6 M€ per la migrazione base e 19,2 M€ per l'intra-migrazione.

v. **Costi aggiuntivi**: i costi aggiuntivi ammontano a € 2,0 milioni e sono relativi al setup infrastrutturale necessario per la messa in funzione del progetto.

w. **Back-up**: i costi per back-up ammontano complessivamente a € 11,2 milioni. Tali costi rappresentano i costi relativi al back-up dei dati, parametrati al numero di server migrati e al costo del Total Cost of Ownership pari a 583 €/TB (ovvero il costo che tiene conto dei costi relativi a hardware, software, gestione e manodopera del servizio). Questi costi sono relativi a servizi forniti da terzi.

x. **G&A**: i costi per G&A esterne ammontano complessivamente a € 125,7 milioni. Tali costi rappresentano i costi amministrativi del PSN, e sono stati stimati sulla base dello studio del benchmark del mercato di riferimento. Questi costi sono relativi a servizi forniti da terzi.

y. **Personale staff**: i costi per personale staff ammontano complessivamente a € 17,4 milioni. Tali costi rappresentano l'incidenza delle strutture organizzative di staff rispetto al totale dei dipendenti. I costi evolvono nel corso della concessione sulla base del personale staff impiegato e dei costi per il personale interno.

La Tabella 3 fornisce una descrizione sintetica delle diverse voci di costo incluse nel PEF.

**TABELLA 3: DESCRIZIONE DEI COSTI OPERATIVI**

| | |
|---|---|
| Spazi attrezzati (esclusi i canoni di affitto) | Canoni annuali per concessione rack attivi |
| Energia | Costi annuali per consumo energetico |
| Connettività | Servizi di supporto tecnico dei clienti di primo livello (interfaccia front end, ticketing, prima risoluzione e indirizzamento |
| Security Operations (SOC + servizi prof.) | Servizio di monitoraggio e controllo della sicurezza cyber delle infrastrutture e dei servizi verso i clienti (h24) |
| Sicurezza (CERT) | Servizio di monitoraggio e controllo preventivo e proattivo dei potenziali incidenti di sicurezza cyber delle infrastrutture |
| Controllo Produzione IT | Servizi di monitoraggio e gestione della produzione IT verso i clienti, supporto tecnico e prima manutenzione / intervento |
| COPS | Servizi di gestione del cliente per Help Desk di 1° livello (COPS) |
| Service management | Servizi di gestione del cliente e monitoraggio dei servizi erogati |
| Sicurezza | Canoni di manutenzione hardware e software relativi ai servizi di sicurezza |
| Manutenzioni | Canoni manutenzione hardware per server, storage ed enclosure, licenze per virtualizzatori / hypervisor |
| Software | Licenze per virtualizzatori/hypervisor Red Hat e Microsoft SPLA |
| Ops tecniche INT | Costi annuali per il personale interno |
| Ops tecniche EXT | Costi annuali per servizi esterni |
| IT infrastructure - service operations | Costi per servizi di infrastruttura del PSN |
| Professional Services | Costi per servizi professionali di sicurezza |
| Secure Public Cloud | Costi per servizi di program governance, design, key management, template, back-up e erogazione del servizio |
| Rearchitect | Costi per servizi relativi all'architettura Cloud |
| Replatform | Costi relativi alla piattaforma Cloud |
| Business & Culture Enablement | Costi relativi formazione/consulenza alle PA |
| Public Cloud PSN Managed | Costi relativi alla fornitura di servizi «Hyperscaler» |
| PaaS Industry | Costi relativi alla messa a disposizione di piattaforme in grado di erogare elementi applicativi e middleware |
| Hybrid Cloud on PSN Site | Costi necessari a offrire servizi del Public Cloud Provider «perimetrati» e installati sull'infrastruttura locale del PSN |
| Servizi di intra-migrazione | Costi della migrazione dei server a partire dal quarto anno della concessione |
| Costi aggiuntivi | Costi per setup infrastrutturale |
| Costi da migrazione | Costi di migrazione (progettazione, analisi infrastrutturale, set-up e migrazione) |
| Back-up | Costo relativo al back-up dei dati |
| | **Costi di struttura** |
| G&A - IT | Costi annuali di amministrazione e gestione IT |
| G&A - Altro | Costi amministrativi annuali |
| Personale Staff | Incidenza strutture organizzative di staff rispetto al totale dei dipendenti |

La tabella seguente riporta l'evoluzione dei costi anno per anno (Tabella 4).

## TABELLA 4: EVOLUZIONE DEI COSTI OPERATIVI

| Costi Operativi (€/mln) | Totale | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Costi diretti** | **(2.293,7)** | **(48,3)** | **(118,7)** | **(154,4)** | **(234,4)** | **(200,2)** | **(215,2)** | **(175,8)** | **(193,9)** | **(202,6)** | **(216,1)** | **(213,8)** | **(181,8)** | **(138,4)** | **-** |
| Connettività | **(65,9)** | (1,3) | (2,1) | (3,5) | (5,0) | (6,0) | (6,1) | (6,2) | (6,3) | (6,5) | (6,6) | (6,4) | (5,5) | (4,4) | - |
| Spazi attrezzati (esclusi canoni di affitto) | **(55,0)** | (1,2) | (1,8) | (3,3) | (5,7) | (5,1) | (5,1) | (5,1) | (5,2) | (5,2) | (5,3) | (5,0) | (4,1) | (3,0) | - |
| Energia | **(105,1)** | (1,2) | (2,9) | (6,1) | (8,3) | (10,1) | (10,2) | (10,1) | (10,1) | (10,3) | (10,5) | (10,1) | (8,5) | (6,4) | - |
| Sicurezza | **(47,1)** | (0,2) | (0,9) | (2,2) | (3,7) | (4,6) | (4,7) | (4,7) | (4,7) | (4,8) | (4,9) | (4,7) | (3,9) | (2,9) | - |
| Manutenzioni | **-** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Software | **(306,0)** | (1,5) | (6,1) | (14,5) | (23,8) | (29,4) | (33,6) | (30,1) | (30,5) | (31,2) | (31,8) | (30,3) | (24,9) | (18,5) | - |
| Ops tecniche INT | **(32,1)** | (1,6) | (2,1) | (3,0) | (2,5) | (2,5) | (2,6) | (2,6) | (2,7) | (2,8) | (2,8) | (2,8) | (2,4) | (1,8) | - |
| Ops tecniche EXT | **(12,9)** | (0,9) | (0,9) | (1,1) | (1,0) | (1,0) | (1,0) | (1,0) | (1,1) | (1,1) | (1,1) | (1,1) | (0,9) | (0,7) | - |
| LAN & WAN Management | **-** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Security Operations (SOC + servizi prof.) | **(96,9)** | (2,5) | (2,7) | (5,7) | (8,7) | (9,2) | (9,0) | (9,0) | (9,1) | (9,3) | (9,4) | (9,0) | (7,5) | (5,7) | - |
| Sicurezza (CERT) | **(6,5)** | (0,1) | (0,2) | (0,3) | (0,6) | (0,6) | (0,6) | (0,6) | (0,7) | (0,7) | (0,7) | (0,6) | (0,5) | (0,3) | - |
| Controllo Produzione IT | **(96,9)** | (0,5) | (1,5) | (3,8) | (6,8) | (8,5) | (9,0) | (9,3) | (9,8) | (10,3) | (10,9) | (10,7) | (9,0) | (6,7) | - |
| COPS | **(98,8)** | (0,3) | (1,6) | (3,9) | (6,8) | (9,0) | (9,3) | (9,6) | (9,9) | (10,5) | (10,9) | (10,8) | (9,1) | (6,9) | - |
| Service management | **(21,0)** | (0,1) | (0,3) | (0,8) | (1,4) | (1,9) | (2,0) | (2,1) | (2,1) | (2,2) | (2,3) | (2,3) | (2,0) | (1,5) | - |
| IT infrastructure - service operations | **(33,3)** | (0,1) | (0,5) | (1,3) | (2,3) | (2,9) | (3,0) | (3,2) | (3,4) | (3,5) | (3,7) | (3,7) | (3,2) | (2,4) | - |
| Servizi professionali di sicurezza | **(77,9)** | (0,4) | (1,8) | (4,5) | (6,6) | (6,7) | (6,8) | (6,9) | (7,1) | (7,2) | (7,3) | (7,4) | (7,5) | (7,6) | - |
| Secure Public Cloud (quota PSN) | **(47,9)** | (1,0) | (1,1) | (1,7) | (2,2) | (3,9) | (4,7) | (4,3) | (4,9) | (4,9) | (5,1) | (5,0) | (4,7) | (4,3) | - |
| Rearchitect | **(182,7)** | (13,8) | (31,4) | (32,1) | (38,0) | (33,3) | (34,1) | - | - | - | - | - | - | - | - |
| Replatform | **(90,7)** | (6,8) | (15,6) | (15,9) | (18,9) | (16,5) | (16,9) | - | - | - | - | - | - | - | - |
| Business & Culture Enablement | **(29,8)** | (0,3) | (1,2) | (2,7) | (3,3) | (2,5) | (2,5) | (2,6) | (2,6) | (2,7) | (2,7) | (2,7) | (2,3) | (1,8) | - |
| Public Cloud PSN Managed (quota PSN) | **(41,2)** | (0,6) | (1,1) | (1,1) | (0,4) | (1,1) | (2,1) | (3,7) | (4,9) | (5,6) | (6,5) | (6,5) | (5,1) | (2,6) | - |
| Secure Public Cloud (rivendita CSP) | **(379,0)** | (1,5) | (6,1) | (14,6) | (24,5) | (31,1) | (32,7) | (34,5) | (36,4) | (38,2) | (40,1) | (40,8) | (39,9) | (38,6) | - |
| Public Cloud PSN Managed (rivendita CSP) | **(195,5)** | - | - | - | (1,9) | (4,9) | (10,0) | (17,6) | (24,2) | (28,2) | (33,5) | (33,9) | (27,0) | (14,4) | - |
| PaaS Industry (quota soci) | **(22,0)** | - | (4,1) | (1,4) | (1,4) | (4,2) | (1,4) | (1,4) | (4,2) | (1,4) | (1,3) | (1,3) | - | - | - |
| PaaS Industry (quota PSN) | **(16,7)** | - | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,7) | (1,6) | - | - | - |
| Hybrid Cloud on PSN Site | **(34,6)** | - | (0,4) | (0,3) | (0,6) | (1,1) | (1,9) | (3,1) | (4,1) | (4,8) | (5,6) | (5,6) | (4,6) | (2,6) | - |
| Hybrid Cloud on PSN site (Quota CSP) | **(39,9)** | - | - | - | (0,4) | (1,0) | (2,0) | (3,6) | (4,9) | (5,8) | (6,8) | (6,9) | (5,5) | (2,9) | - |
| Servizi di intra-migrazione | **(19,2)** | - | - | - | (0,2) | (0,4) | (0,9) | (1,7) | (2,3) | (2,7) | (3,3) | (3,4) | (2,8) | (1,5) | - |
| Costi aggiuntivi | **(2,0)** | - | (2,0) | - | - | - | - | - | - | - | - | - | - | - | - |
| Costi da migrazione | **(125,6)** | (12,2) | (27,9) | (28,5) | (57,0) | - | - | - | - | - | - | - | - | - | - |
| Back-up | **(11,2)** | (0,1) | (0,2) | (0,5) | (0,9) | (1,1) | (1,1) | (1,1) | (1,1) | (1,1) | (1,2) | (1,1) | (0,9) | (0,7) | - |
| **Costi indiretti** | **(143,1)** | **(1,4)** | **(3,6)** | **(7,4)** | **(10,7)** | **(12,7)** | **(13,2)** | **(13,5)** | **(13,9)** | **(14,5)** | **(14,9)** | **(14,8)** | **(12,7)** | **(9,8)** | **-** |
| G&A - IT | **(95,9)** | (0,5) | (1,9) | (4,4) | (6,9) | (8,6) | (9,0) | (9,2) | (9,6) | (10,0) | (10,4) | (10,2) | (8,7) | (6,6) | - |
| G&A - Altro | **(29,8)** | (0,5) | (1,0) | (2,0) | (2,3) | (2,6) | (2,7) | (2,7) | (2,8) | (2,9) | (2,9) | (2,9) | (2,5) | (2,0) | - |
| Personale Staff | **(17,4)** | (0,4) | (0,7) | (1,0) | (1,5) | (1,5) | (1,5) | (1,6) | (1,6) | (1,6) | (1,6) | (1,6) | (1,5) | (1,2) | - |

Fonte: PEF, Conto Economico.

# VI. Operating Leases

27. I costi operativi del PSN includono inoltre i canoni annuali per l'affitto degli spazi attrezzati all'interno dei data center. In linea col principio contabile IFRS 16, il PEF capitalizza questi costi nello stato patrimoniale come *operating lease liabilities*. Più in dettaglio:

    a. Il PEF prevede un esborso per i canoni di affitto dei data center complessivamente pari a € 85,3 milioni nel corso della concessione. Lo spazio affittato è modulato in funzione della percentuale di migrazione per ciascun data center e per tutti gli anni della concessione, mentre il canone d'affitto unitario è definito in funzione delle specifiche tecniche dei data center (Tier III vs Tier IV).

    b. I pagamenti attesi per i canoni di affitto sono attualizzati e iscritti nel passivo dello stato patrimoniale alla voce "**Debiti per leasing (data center)**" assumendo un tasso di finanziamento del PSN pari al 2,7%. In contropartita al debito, il diritto di utilizzo dei data center (c.d. *right of use*) è iscritto nell'attivo dello stato patrimoniale alla voce "**Diritti d'uso (data center)**".

    c. Successivamente alla rilevazione iniziale, il Diritto d'uso è ridotto per le quote di ammortamento annue. Tali quote sono costanti, seguono la durata del contratto e sono contabilizzate nel Conto Economico alla voce "**Ammortamento diritti d'uso**". Gli interessi pagati sulla *lease liabilty* sono iscritti nella voce di Conto Economico "**Oneri finanziari - Debiti per leasing**".

# VII. Tariffe e Ricavi

28. Il PEF prevede l'erogazione dei servizi previsti nel bando di gara sulla base dei prezzi di listino che sono stati offerti dalla cordata Fastweb-Aruba, per cui è stata proposta un'offerta equivalente sulla base del diritto di prelazione spettante al raggruppamento in qualità di promotore.

29. Il PEF procede al calcolo dei ricavi annuali sulla base dei valori di listino.

30. Le seguenti tabelle mostrano i prezzi di listino applicati (Tabella 5) e l'andamento dei ricavi (Tabella 6) per tipologia di servizio nel corso della concessione. Nella prima colonna viene individuato il listino di riferimento, nella seconda il tipo di servizio offerto, nella terza e nella quarta sono elencate i prezzi e le quantità poste a base di gara e nella quinta i prezzi offerti dal RTI e sulla base dei quali è stato costruito il PEF.

## TABELLA 5: PREZZI DI LISTINO

| Numero Listino | Tipologia | Elemento | Quantità | Canone Annuale | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 1 | IaaS Private (HA) | Blade Medium | 45.321 | 11.083 € | 4.987 € |
| Listino 1 | IaaS Private (HA) | Blade Large | 7.558 | 15.922 € | 8.040 € |
| Listino 1 | IaaS - Storage (HA) | Storage High Performance | 18.145 | 721 € | 364 € |
| Listino 1 | IaaS - Storage (HA) | Storage Standard Performance | 27.217 | 395 € | 199 € |
| Listino 1 | IaaS - Storage (HA) | NAS | 9.072 | 395 € | 375 € |
| Listino 1 | IaaS - Storage (HA) | Object storage | 18.145 | 395 € | 199 € |
| Listino 1 | IaaS - Storage (HA) | Storage HP Encrypted | 9.072 | 988 € | 499 € |
| Listino 1 | IaaS - Storage (HA) | Storage SP Encrypted | 9.072 | 652 € | 329 € |
| Listino 1 | IaaS Shared (HA) | VM Tiny | 127.055 | 544 € | 275 € |
| Listino 1 | IaaS Shared (HA) | VM Small | 95.296 | 1.077 € | 431 € |
| Listino 1 | IaaS Shared (HA) | VM Medium | 63.527 | 2.082 € | 833 € |
| Listino 1 | IaaS Shared (HA) | VM Large | 23.826 | 3.844 € | 1.537 € |
| Listino 1 | IaaS Shared (HA) | VM X-Large | 7.942 | 7.352 € | 4.779 € |
| Listino 1 | IaaS Shared (HA) | Pool Small | 7.942 | 2.973 € | 1.501 € |
| Listino 1 | IaaS Shared (HA) | Pool Medium | 7.942 | 5.435 € | 2.744 € |
| Listino 1 | IaaS Shared (HA) | Pool Large | 3.966 | 10.529 € | 4.738 € |
| Listino 1 | IaaS Shared (HA) | Pool XLarge | 992 | 19.310 € | 10.621 € |
| Listino 1 | CaaS | Licensed - Medium | 2.000 | 8.888 € | 4.488 € |
| Listino 1 | CaaS | Licensed - Large | 1.005 | 21.107 € | 10.659 € |
| Listino 1 | CaaS | Open Source (vCPU/anno) | 2.000 | 889 € | 449 € |
| Listino 1 | PaaS - DB | Mysql | 18.886 | 1.900 € | 1.520 € |
| Listino 1 | PaaS - DB | PostgreSQL | 19.327 | 1.857 € | 1.486 € |
| Listino 1 | PaaS - DB | SQL server | 4.534 | 5.394 € | 4.315 € |
| Listino 1 | PaaS - DB | Oracle dbms - Enterprise | 308 | 26.471 € | 13.368 € |
| Listino 1 | PaaS - DB | Oracle dbms - Standard | 1.375 | 11.873 € | 5.996 € |
| Listino 1 | PaaS - DB | MongoDB | 1.559 | 6.261 € | 3.162 € |
| Listino 1 | PaaS - DB | MariaDB | 17.265 | 1.891 € | 955 € |
| Listino 1 | PaaS - Big Data | Data Lake - 1TB | 5.468 | 593 € | 299 € |
| Listino 1 | PaaS - Big Data | Batch/Real time Processing - 1 Worker | 1.094 | 13.924 € | 7.032 € |
| Listino 1 | PaaS - Big Data | Event Message - 1 Worker | 273 | 6.666 € | 3.366 € |
| Listino 1 | PaaS - Big Data | Data Governance | 182 | 5.925 € | 5.333 € |
| Listino 1 | Sistemi operativi | Windows Server STD CORE (2 core) | 262.815 | 129 € | 117 € |
| Listino 1 | Sistemi operativi | Red Hat per VM | 100.899 | 604 € | 544 € |
| Listino 1 | Sistemi operativi | Red Hat per Bare Metal | 33.446 | 1.079 € | 971 € |
| Listino 1 | Data Protection | Opzione DR | 125.696.242 | 84% | 65% |
| Listino 1 | Data Protection | Backup | - | 642 € | 324 € |
| Listino 1 | Data Protection | Golden copy | - | 770 € | 389 € |
| Listino 1 | Multicloud | CMP per server | - | 148 € | 75 € |
| Listino 1 | Security | Antivirus | - | 829 € | 419 € |
| Listino 1 | IaaS Shared | VM Tiny | - | 348 € | 176 € |
| Listino 1 | IaaS Shared | VM Small | - | 722 € | 289 € |
| Listino 1 | IaaS Shared | VM Medium | - | 1.415 € | 566 € |
| Listino 1 | IaaS Shared | VM Large | - | 2.629 € | 1.052 € |
| Listino 1 | IaaS Shared | VM X-Large | - | 5.046 € | 3.280 € |
| Listino 1 | IaaS Shared | Pool Small | - | 1.951 € | 985 € |
| Listino 1 | IaaS Shared | Pool Medium | - | 3.545 € | 1.790 € |
| Listino 1 | IaaS Shared | Pool Large | - | 7.033 € | 3.165 € |
| Listino 1 | IaaS Shared | Pool XLarge | - | 12.843 € | 7.064 € |
| Listino 1 | IaaS Private | Blade Medium | - | 7.778 € | 3.928 € |
| Listino 1 | IaaS Private | Blade Large | - | 11.172 € | 5.642 € |
| Listino 1 | IaaS Shared (HA) | Pool - 1GB ram aggiuntivo | - | 64 € | 32 € |
| Listino 1 | IaaS Shared (HA) | Pool - 1vCPU aggiuntiva | - | 126 € | 64 € |
| Listino 1 | IaaS Shared | Pool - 1GB ram aggiuntivo | - | 45 € | 23 € |
| Listino 1 | IaaS Shared | Pool - 1vCPU aggiuntiva | - | 88 € | 44 € |
| Listino 1 | Connettività | Connessione dedicata 1 Gbps | - | 86.942 € | 8.694 € |

| | Tipologia | Elemento | Quantità | Canone Annuale | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 1 | Compute | Server 2-processore 26 core 768 GB RAM 24 TB Disco (o equivalente) | 3.089 | 57.883 € | 53.832 € |
| Listino 1 | Policy | Server | 33.393 | 86 € | 80 € |
| Listino 1 | Kubernetes | vCPU | 53.428 | 29 € | 27 € |
| Listino 1 | SQL Data services | vCPU | 10.018 | 2.213 € | 2.058 € |
| Listino 1 | Monitoring | GB | 14.609 | 1.322 € | 1.230 € |

| | Tipologia | Elemento | Quantità | Canone Annuale | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 1 | **Progetto Cloud 1** | | 694 | 550.531 € | 511.994 € |
| Listino 1 | **Progetto Cloud 2** | | 477 | 342.591 € | 318.610 € |

| | Tipologia | Elemento | Quantità | Canone Annuale | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 1 | **CLUSTER 1** | | 67 | 590.778 € | 413.545 € |
| Listino 1 | **CLUSTER 2** | | 96 | 490.747 € | 343.523 € |
| Listino 1 | **CLUSTER 3** | | 96 | 500.359 € | 350.251 € |
| Listino 1 | **CLUSTER 4** | | 96 | 1.113.436 € | 779.405 € |
| Listino 1 | **CLUSTER 5** | | 91 | 918.730 € | 643.111 € |

| | Tipologia | Elemento | Quantità | Canone Annuale | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 2 | Housing | Rack | 4.774 | 16.693 € | 15.374 € |
| Listino 2 | Hosting | Server (1RU) | 47.253 | 10.674 € | 4.804 € |
| Listino 2 | Hosting | Server su rack dedicato (1RU) | 11.816 | 13.801 € | 6.456 € |
| Listino 2 | Hosting - Storage | Storage High Performance | 6.968 | 360 € | 138 € |
| Listino 2 | Hosting - Storage | Storage Standard Performance | 10.451 | 198 € | 138 € |
| Listino 2 | Hosting - Storage | NAS | 3.484 | 198 € | 138 € |
| Listino 2 | Hosting - Storage | Object storage | 6.968 | 198 € | 162 € |
| Listino 2 | Hosting - Storage | Storage HP Encrypted | 3.484 | 494 € | 138 € |
| Listino 2 | Hosting - Storage | Storage SP Encrypted | 3.484 | 326 € | 138 € |
| Listino 2 | Housing | Potenza elettrica aggiuntiva (pacchetto da 1kW di targa) | - | 1.384 € | 1.384 € |
| Listino 2 | Housing | Rilancio connettività (fibra monomodale) | - | 183 € | 109 € |
| Listino 2 | Housing | IP Pubblico singolo | - | 40 € | 24 € |
| Listino 2 | Housing | IP Pubblici /29 (8 indirizzi) | - | 110 € | 65 € |
| Listino 2 | Housing | Cage | - | 570 € | 339 € |
| Listino 2 | Housing | Housing router in sala TLC | - | 3.534 € | 2.103 € |
| Listino 2 | Housing | Moving server | - | 4.000 € | 2.380 € |
| Listino 2 | PaaS - AI | AI Platform - 1 Worker - 1 GPU | 729 | 24.886 € | 14.807 € |
| Listino 2 | PaaS - AI | Semantic Knowledge Search - 1 Worker | 1.094 | 4.740 € | 2.820 € |
| Listino 2 | PaaS - AI | Text Analytics /NLP - 1 Worker | 365 | 7.643 € | 4.548 € |
| Listino 2 | PaaS - AI | Audio Analytics - 1 flusso audio H24 X 365G | 911 | 4.266 € | 2.538 € |
| Listino 2 | PaaS - AI | Video Analytics - 1 flusso video H24 X 365G | 1.823 | 12.591 € | 7.492 € |
| Listino 2 | PaaS - Spid Enabling & Profiling | Spid Enabling & Profiling 100 Utenti | 1.823 | 9.777 € | 5.817 € |

| | Tipologia Priorità 2 | Figura | Quantità | Canone | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 2 | Figura professionale | Project Manager (tariffa giorno/persona) | 103.167 | 465 € | 372 € |
| Listino 2 | Figura professionale | Cloud Application Architect (tariffa giorno/persona) | 55.297 | 651 € | 387 € |
| Listino 2 | Figura professionale | UX Designer (tariffa giorno/persona) | 46.015 | 372 € | 297 € |
| Listino 2 | Figura professionale | Business Analyst (tariffa giorno/persona) | 46.015 | 372 € | 297 € |
| Listino 2 | Figura professionale | DevOps Expert (tariffa giorno/persona) | 92.029 | 391 € | 313 € |
| Listino 2 | Figura professionale | Database Specialist and Administrator (tariffa giorno/persona) | 78.854 | 419 € | 249 € |
| Listino 2 | Business & Culture Eneblement Figura professionale | Developer (Cloud/Mobile/Front-End Developer) (tariffa giorno/persona) | 206.005 | 233 € | 186 € |
| Listino 2 | Figura professionale | System Integrator & Testing Specialist (tariffa giorno/persona) | - | 353 € | 282 € |
| Listino 2 | Figura professionale | System and Network Administrator (tariffa giorno/persona) | 136.154 | 372 € | 297 € |
| Listino 2 | Figura professionale | Cloud Application Specialist (tariffa giorno/persona) | 125.286 | 530 € | 315 € |
| Listino 2 | Figura professionale | Cloud Security Specialist (tariffa giorno/persona) | 77.110 | 419 € | 249 € |
| Listino 2 | Figura professionale | Enterprise Architect (tariffa giorno/persona) | 46.015 | 698 € | 415 € |
| Listino 2 | Figura professionale | Security Principal (tariffa giorno/persona) | 9.282 | 651 € | 521 € |
| Listino 2 | Figura professionale | Senior Information Security Consultant (tariffa giorno/persona) | 9.282 | 530 € | 424 € |
| Listino 2 | Figura professionale | Junior Information Security Consultant (tariffa giorno/persona) | 14.851 | 372 € | 297 € |
| Listino 2 | Figura professionale | Security Solution Architect (tariffa giorno/persona) | 18.563 | 530 € | 424 € |
| Listino 2 | Figura professionale | Senior Security Auditor/Analyst (tariffa giorno/persona) | 40.839 | 558 € | 446 € |
| Listino 2 | Figura professionale | Junior Security Analyst (tariffa giorno/persona) | 18.563 | 353 € | 282 € |
| Listino 2 | Figura professionale | Senior Penetration Tester (tariffa giorno/persona) | 7.426 | 465 € | 372 € |
| Listino 2 | Figura professionale | Junior Penetration Tester (tariffa giorno/persona) | 11.138 | 326 € | 261 € |
| Listino 2 | Figura professionale | Forensic Expert (tariffa giorno/persona) | 7.426 | 465 € | 372 € |
| Listino 2 | Figura professionale | Data Protection Specialist (tariffa giorno/persona) | 12.994 | 465 € | 372 € |
| Listino 2 | Figura professionale | Systems Architect (tariffa giorno/persona) | 8.283 | 605 € | 484 € |
| Listino 2 | Business & Culture Eneblement Figura professionale | Product/Network/Technical Specialist (tariffa giorno/persona) | 84.530 | 419 € | 335 € |
| Listino 2 | Business & Culture Eneblement Figura professionale | Educational Designer/Tutoring (tariffa giorno/persona) | 14.632 | 372 € | 297 € |
| Listino 2 | Business & Culture Enablement | Costo adesione al servizio per Amministrazione | 70 | 38.588 € | 22.960 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 0 a 1.000 | 2.593 | 226 € | 226 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 1.001 a 5.000 | 239 | 453 € | 453 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 5.001 a 10.000 | 239 | 679 € | 679 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 10.001 a 20.000 | 12 | 1.019 € | 1.019 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 20.001 a 50.000 | 12 | 1.585 € | 1.585 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 50.001 a 100.000 | 12 | 2.377 € | 2.377 € |
| Listino 2 | Business & Culture Enablement | Canone settimanale per fascia utenti da 100.001 a 150.000 | 12 | 3.170 € | 3.170 € |
| Listino 2 | Business & Culture Enablement | Corso bassa interattività | 159 | 3.483 € | 1.915 € |
| Listino 2 | Business & Culture Enablement | Corso media interattività | 159 | 4.937 € | 2.715 € |
| Listino 2 | Business & Culture Enablement | Corso alta interattività | 159 | 6.503 € | 3.577 € |
| Listino 2 | Business & Culture Enablement | A catalogo | 159 | 5.500 € | 5.500 € |

| | Tipologia MIGRAZIONE | Figura | Quantità | Canone | Canone Annuale Scontato |
|---|---|---|---|---|---|
| Listino 3 | Figura professionale | Cloud Application Architect (tariffa giorno/persona) | 50.407 | 651 € | 387 € |
| Listino 3 | Figura professionale | Database Specialist and Administrator (tariffa giorno/persona) | 75.611 | 419 € | 249 € |
| Listino 3 | Figura professionale | System Integrator & Testing Specialist (tariffa giorno/persona) | 151.222 | 353 € | 210 € |
| Listino 3 | Figura professionale | Cloud Application Specialist (tariffa giorno/persona) | 100.814 | 530 € | 315 € |
| Listino 3 | Figura professionale | Cloud Security Specialist (tariffa giorno/persona) | 75.611 | 419 € | 249 € |
| Listino 3 | Figura professionale | Enterprise Architect (tariffa giorno/persona) | 50.407 | 698 € | 415 € |

Fonte: PEF, Listino quantità per servizio.

### TABELLA 6: EVOLUZIONE DEI RICAVI DURANTE LA CONCESSIONE

| Ricavi (€/mln) | Totale | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Housing | **79,9** | 0,4 | 1,6 | 3,9 | 6,5 | 8,1 | 8,1 | 8,0 | 8,0 | 8,1 | 8,1 | 7,8 | 6,6 | 4,8 | - |
| Hosting | **336,1** | 1,5 | 6,3 | 15,2 | 25,5 | 32,0 | 32,7 | 33,1 | 33,7 | 34,8 | 35,8 | 34,7 | 29,2 | 21,4 | - |
| IaaS Private | **327,5** | 1,4 | 5,9 | 14,3 | 23,9 | 30,1 | 31,2 | 31,8 | 32,8 | 34,2 | 35,5 | 34,6 | 29,1 | 22,5 | - |
| IaaS Shared | **305,3** | 1,3 | 5,5 | 13,3 | 22,3 | 28,1 | 29,0 | 29,7 | 30,6 | 31,9 | 33,1 | 32,3 | 27,2 | 21,0 | - |
| Altri servizi di IaaS e Cloud | **233,0** | 0,9 | 3,8 | 9,2 | 15,6 | 19,9 | 21,1 | 22,4 | 23,8 | 25,2 | 26,8 | 26,3 | 22,0 | 15,9 | - |
| Hybrid Cloud on PSN Site | **232,0** | - | - | - | 2,1 | 5,4 | 11,3 | 20,2 | 28,0 | 33,2 | 39,9 | 41,0 | 33,0 | 17,8 | - |
| Public Cloud PSN Managed | **252,1** | - | - | - | 2,3 | 5,9 | 12,3 | 22,0 | 30,5 | 36,1 | 43,4 | 44,5 | 35,9 | 19,4 | - |
| Secure Public Cloud | **556,8** | 2,0 | 8,3 | 19,9 | 33,9 | 43,5 | 46,4 | 49,7 | 53,1 | 56,5 | 60,1 | 61,9 | 61,4 | 60,2 | - |
| PaaS Industry | **57,2** | - | 5,4 | 5,5 | 5,6 | 5,6 | 5,7 | 5,8 | 5,8 | 5,9 | 5,9 | 6,0 | - | - | - |
| Sistemi operativi | **128,8** | 0,6 | 2,3 | 5,6 | 9,4 | 11,9 | 12,2 | 12,5 | 12,9 | 13,5 | 14,0 | 13,6 | 11,5 | 8,9 | - |
| Ricavi da migrazione | **147,4** | 12,7 | 28,8 | 29,1 | 58,0 | 0,4 | 0,9 | 1,6 | 2,3 | 2,7 | 3,2 | 3,3 | 2,7 | 1,5 | - |
| **Ricavi da servizi core** | **2.656,2** | **21,0** | **68,0** | **116,0** | **205,2** | **191,1** | **211,1** | **236,9** | **261,4** | **282,0** | **305,8** | **305,9** | **258,5** | **193,4** | **-** |
| Professional Services | **76,5** | 0,5 | 1,9 | 4,5 | 6,6 | 6,7 | 6,8 | 6,9 | 6,9 | 7,0 | 7,1 | 7,1 | 7,2 | 7,3 | - |
| Rearchitect | **184,8** | 14,3 | 32,2 | 32,6 | 38,4 | 33,4 | 34,0 | - | - | - | - | - | - | - | - |
| Replatform | **91,8** | 7,1 | 16,0 | 16,2 | 19,1 | 16,6 | 16,9 | - | - | - | - | - | - | - | - |
| Business & Culture Enablement | **27,6** | 0,3 | 1,0 | 2,3 | 2,9 | 2,4 | 2,4 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,1 | 1,6 | - |
| IT infrastructure - service operations | **32,7** | 0,1 | 0,6 | 1,3 | 2,3 | 2,9 | 3,0 | 3,1 | 3,3 | 3,5 | 3,6 | 3,6 | 3,0 | 2,3 | - |
| **Totale Ricavi** | **3.069,5** | **43,2** | **119,7** | **173,0** | **274,4** | **253,0** | **274,2** | **249,3** | **274,1** | **295,0** | **319,0** | **319,1** | **270,9** | **204,7** | **-** |

Fonte: PEF, Conto Economico.

# VIII. Ipotesi macroeconomiche, fiscali e capitale circolante

31. **Inflazione:** Ai fini dell'adeguamento inflattivo nello sviluppo dei dati economico-finanziari prospettici, il PEF considera la curva inflattiva stimata da IHS Markit come segue:

    a. I ricavi vengono inflazionati con una ponderazione dell'85% del 75% della curva di inflazione utilizzata sulla base di quanto rappresentato al punto di cui sopra, sulla base di quanto definito nell'addendum allo schema di convenzione, che prevede che i prezzi applicati alle amministrazioni verranno adeguati al 75% della variazione annuale dell'indice ISTAT dei prezzi al consumo delle famiglie di operai e impiegati senza tabacchi, fermo restando il rispetto dell'equilibrio economico-finanziario.

    b. I costi sostenuti dal PSN e relativi a servizi da terzi vengono inflazionati con una ponderazione del 100% sulla base della curva di inflazione di IHS Markit, ad eccezione dei costi aggiuntivi e dell'energia per cui sono state fatte ipotesi puntuali di sostenimento dei costi.

    c. Le capex vengono inflazionate con una ponderazione del 100% della curva IHS Markit.

    La tabella seguente mostra l'andamento della curva inflattiva utilizzata.

**TABELLA 7: EVOLUZIONE DEI RICAVI DURANTE LA CONCESSIONE**

| | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GDP deflators | 110,7727 | 113,7078 | 115,987 | 118,5086 | 120,8106 | 122,8037 | 124,8818 | 126,9506 | 129,0294 | 130,974 | 133,0102 | 135,1957 | 137,4013 | 139,6889 |
| **YoY %** | | **2,6%** | **2,0%** | **2,2%** | **1,9%** | **1,6%** | **1,7%** | **1,7%** | **1,6%** | **1,5%** | **1,6%** | **1,6%** | **1,6%** | **1,7%** |
| YoY % ponderazione 75% | | 2,0% | 1,5% | 1,6% | 1,5% | 1,2% | 1,3% | 1,2% | 1,2% | 1,1% | 1,2% | 1,2% | 1,2% | 1,2% |
| Crescita cumulata 100% | | 2,6% | 4,7% | 7,0% | 9,1% | 10,9% | 12,7% | 14,6% | 16,5% | 18,2% | 20,1% | 22,0% | 24,0% | 26,1% |
| Crescita cumulata 75% | | 2,0% | 3,5% | 5,2% | 6,7% | 8,1% | 9,4% | 10,8% | 12,2% | 13,4% | 14,7% | 16,2% | 17,6% | 19,0% |

Fonte: IHS Markit

32. **Tassi di interesse:** Nel PEF si prevede l'applicazione di un tasso IRS pari a 0,6%.

33. **Curva Euribor:** nel PEF ai fini del calcolo degli interessi sulle linee di debito viene utilizzata la curva Euribor estratta in data 10.03.2022, che presenta il seguente andamento:

**TABELLA 8: EVOLUZIONE DELLA CURVA EURIBOR**

| | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Curva Euribor | 0,2% | 0,6% | 0,7% | 0,8% | 1,0% | 1,1% | 1,2% | 1,3% | 1,4% | 1,4% | 1,5% | 1,3% | 1,3% | 1,3% |

34. **Imposta sul valore aggiunto (IVA):** I costi e gli investimenti sono soggetti ad una aliquota IVA pari al 22% del costo imponibile.

35. **Split payment:** Essendo i servizi rivolti ad Ente Pubblico, ai fini IVA, i canoni percepiti sono soggetti al regime dello Split Payment, che prevede che il versamento dell'IVA sia assolto dell'Ente Pubblico, pertanto tale valore non rappresenta per il Concessionario né un credito verso l'Ente Pubblico né un debito verso l'Erario.

36. **Imposte:** Il PEF calcola le imposte sul reddito d'esercizio applicando le aliquote fiscali IRES e IRAP vigenti, calcolando anche le deduzioni applicabili alle imposte dirette, mantenute costanti per tutta la durata della concessione. In particolare, è applicata un'aliquota IRES pari al 24%, e una aliquota IRAP pari al 4,82%, pari all'aliquota IRAP della Regione Lazio. Il PEF prevede un meccanismo di loss carry forward che permette la deduzione dal reddito d'esercizio delle perdite degli anni precedente in linea con la normativa vigente.

37. **Capitale circolante:** Il PEF assume i seguenti tempi medi di incasso e pagamento:

    a. Incasso crediti commerciali: 120 giorni;

    b. Pagamento debiti commerciali: 120 giorni;

    c. Pagamento personale: 30 giorni.

# IX. Ipotesi Finanziarie

38. Il PEF è stato redatto introducendo una serie di ipotesi finanziarie relative al capitale sociale iniziale, alle iniezioni di capitale proprio da parte dei soci, e al ricorso al finanziamento da terzi e al relativo tasso di interesse sul debito.

39. **Capitale Sociale e riserve**: Il PEF prevede un capitale sociale iniziale pari a € 3.0 milioni e la costituzione di una riserva versamento soci. La riserva viene distribuita lungo il corso della concessione nel rispetto dei vincoli legati alla riserva legale obbligatoria e al mantenimento di un patrimonio netto positivo.

40. **Distribuzioni:** Le distribuzioni di riserve e dividendi sono previste in presenza di cassa disponibile e dipendono dall'ammontare delle riserve distribuibili.

41. **Finanziamenti di terzi:** Per far fronte alla copertura del fabbisogno finanziario, espresso dal valore degli investimenti e degli oneri finanziari al netto della cassa operativa a disposizione e della riserva versamento soci, il PEF prevede il ricorso a finanziamenti da terzi in funzione del debito massimo sostenibile con un DSCR di 1,4x ed una durata del finanziamento di 7,5 anni, risultando in una copertura del 62% del fabbisogno complessivo. In particolare, il PEF prevede che il debito finanziario abbia le seguenti caratteristiche:

    a. costo iniziale di emissione (inclusivo dell'imposta sostitutiva dello 0,25%) del 2,75%

    b. commitment fee pari al 35% dello spread

    c. periodo di disponibilità di 4 anni (dal primo al quarto anno di concessione)

    d. periodo di rimborso di 7,5 anni, prevedendo pertanto 18 mesi di coda rispetto alla fine della concessione

    e. profilo di rimborso a rate variabili "scolpite" nel rispetto di un Debt Service Coverage Ratio ("DSCR") di 1,40x

    f. tasso di interesse composto da (i) Euribor 6 mesi con hedging al 75% (ii) IRS pari a 0,6% (iii) costo dello swap pari a 0,2% (iv) spread del 2,7%

    g. DSRA pari al servizio del debito dei sei mesi successivi periodo per periodo

    La Tabella  riporta l'evoluzione del ricorso al finanziamento per far fronte al fabbisogno finanziario del progetto.

**TABELLA 9: PROSPETTO FONTI E IMPIEGHI DEL PSN**

| | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Impieghi** | | | | | | | | | | | | | | |
| **Liquidità immediate** | **-** | **13,8** | **21,7** | **76,6** | **73,9** | **69,0** | **55,3** | **30,8** | **22,5** | **22,5** | **22,5** | **-** | **-** | **-** |
| Cassa e Disponibilità liquide | - | 13,8 | 21,7 | 21,7 | 9,2 | 12,5 | 10,7 | - | - | - | - | - | - | - |
| MRA + DSRA | - | - | - | 54,8 | 64,7 | 56,5 | 44,7 | 30,8 | 22,5 | 22,5 | 22,5 | - | - | - |
| **Liquidità differite** | **38,3** | **73,9** | **102,5** | **152,5** | **133,2** | **146,9** | **130,4** | **145,4** | **151,7** | **158,9** | **157,3** | **133,5** | **101,4** | **-** |
| Crediti commerciali | 14,2 | 39,3 | 56,9 | 90,2 | 83,2 | 90,1 | 82,0 | 90,1 | 97,0 | 104,9 | 104,9 | 89,1 | 67,3 | - |
| Crediti tributari | 24,1 | 34,6 | 45,6 | 62,2 | 50,0 | 56,8 | 48,5 | 55,3 | 54,8 | 54,0 | 52,4 | 44,4 | 34,1 | - |
| Ratei e Risconti | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Rimanenze** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Capitale d'esercizio** | **38,3** | **87,7** | **124,2** | **229,0** | **207,1** | **215,9** | **185,8** | **176,2** | **174,3** | **181,5** | **179,9** | **133,5** | **101,4** | **-** |
| **Immobilizzazioni tecniche** | **94,0** | **111,8** | **131,2** | **133,2** | **107,8** | **97,5** | **89,6** | **95,3** | **90,2** | **68,6** | **44,4** | **22,4** | **6,2** | **1,8** |
| **Immobilizzazioni immateriali** | **48,5** | **44,6** | **40,6** | **36,7** | **32,7** | **28,8** | **24,8** | **20,9** | **16,9** | **12,9** | **9,0** | **5,0** | **1,1** | **-** |
| **Immobilizzazioni finanziarie** | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| **Immobilizzazioni nette** | **142,5** | **156,4** | **171,9** | **169,9** | **140,5** | **126,2** | **114,4** | **116,2** | **107,1** | **81,6** | **53,4** | **27,4** | **7,2** | **1,8** |
| **Capitale Investito** | **180,8** | **244,1** | **296,1** | **398,9** | **347,6** | **342,1** | **300,2** | **292,4** | **281,4** | **263,0** | **233,3** | **160,9** | **108,7** | **1,8** |
| **Fonti** | | | | | | | | | | | | | | |
| **Passività correnti** | **110,4** | **143,9** | **165,3** | **204,1** | **175,3** | **181,0** | **153,6** | **160,0** | **155,9** | **153,1** | **143,7** | **117,5** | **84,9** | **0,0** |
| Debiti finanziari a breve termine | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Debiti per leasing (data center) | 69,3 | 68,4 | 65,1 | 59,3 | 53,3 | 47,2 | 40,9 | 34,5 | 27,9 | 21,1 | 14,3 | 7,2 | 0,0 | 0,0 |
| Debiti commerciali | 16,9 | 40,9 | 54,5 | 82,6 | 72,0 | 77,1 | 64,2 | 70,3 | 73,3 | 77,9 | 77,0 | 65,9 | 50,8 | - |
| Ratei e Risconti | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| Linea IVA | 24,1 | 34,6 | 45,6 | 62,2 | 50,0 | 56,8 | 48,5 | 55,3 | 54,8 | 54,0 | 52,4 | 44,4 | 34,1 | - |
| **Passività consolidate** | **59,6** | **89,4** | **120,0** | **171,6** | **169,3** | **160,0** | **143,6** | **125,4** | **97,0** | **58,2** | **18,0** | **0,1** | **0,1** | **-** |
| Debiti finanziari a lungo termine | 59,6 | 89,3 | 119,9 | 171,4 | 169,2 | 159,9 | 143,5 | 125,3 | 96,8 | 58,1 | 17,9 | - | - | - |
| Altri Debiti | 0,0 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | 0,1 | - |
| **Capitale netto** | **10,8** | **10,8** | **10,8** | **23,2** | **3,0** | **1,1** | **3,0** | **7,0** | **28,5** | **51,8** | **71,5** | **43,2** | **23,6** | **1,8** |
| Capitale sociale | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 | 3,0 |
| Riserva versamento soci | 26,0 | 54,3 | 77,1 | 102,2 | 89,2 | 89,2 | 78,3 | 62,3 | 52,7 | 48,2 | 48,2 | 39,6 | 20,0 | 4,3 |
| Riserva Legale | - | - | - | - | - | - | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 | 0,6 |
| Utili (perdite) portati a nuovo | (18,2) | (46,5) | (69,3) | (82,0) | (89,2) | (91,1) | (78,9) | (58,9) | (27,8) | - | 19,8 | - | - | (6,1) |
| **Capitale di finanziamento** | **180,8** | **244,1** | **296,1** | **398,9** | **347,6** | **342,1** | **300,2** | **292,4** | **281,4** | **263,0** | **233,3** | **160,9** | **108,7** | **1,8** |

Fonte: PEF, Prospetto Fonti Impieghi.

42. **Finanziamento IVA**: Il PEF prevede anche l'erogazione di una linea IVA per far fronte al fabbisogno IVA generato su costi e capex durante la concessione, con le seguenti caratteristiche:

    a. costo iniziale di emissione (inclusivo dell'imposta sostitutiva dello 0,25%) del 2,75%

    b. commitment fee pari al 35% dello spread

    c. tasso di interesse composto da (i) Euribor 6 mesi con hedging al 75% (ii) IRS pari a 0,6% (iii) costo dello swap pari a 0,2% (iv) spread del 2,4%

43. **MRA:** Per far fronte agli investimenti degli anni 5, 6, 7 e 8 della concessione, il PEF prevede la costituzione di un Maintenance Reserve Account ("MRA"), finanziato per € 49,8 milioni al quarto anno di concessione e alimentato da accantonamenti sui flussi di cassa al quinto anno della concessione per il 70% del flusso di cassa disponibile per l'autofinanziamento.

# X. Indicatori dell'Equilibrio Economico-Finanziario

44. Il PEF esprime l'Equilibrio Economico-Finanziario del PSN sulla base di due indicatori specifici della redditività e bancabilità del progetto:

    a. **Il tasso interno di rendimento del progetto (TIR di progetto):** Il PEF prevede un TIR di progetto al lordo delle imposte pari al 7,7%, e un TIR di progetto al netto delle imposte pari al 5,1%. Tale valore del TIR di progetto risulta in linea con la redditività attesa per progetti di simile rischio, misurati in termini di costo medio ponderato del capitale.

    b. **Il DSCR minimo**: il PEF prevede il rimborso del finanziamento sulla base di un DSCR minimo pari a 1,40. Tale valore del DSCR è in linea con gli *standard* di bancabilità richiesti dalle banche finanziatrici per il finanziamento di progetti di simile rischio.

    La Tabella riporta l'andamento dei flussi di cassa utilizzati per il calcolo del TIR di progetto e il valore del DSRC in ogni anno della concessione.

**TABELLA 10: EVOLUZIONE DEGLI INDICI DURANTE LA CONCESSIONE**

| Indicatori di Equilibrio economico-finanziario | | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Totale flussi di cassa, lordo imposte** | - | **(109,7)** | **(49,7)** | **(50,5)** | **(81,5)** | **26,5** | **17,7** | **43,6** | **31,0** | **54,2** | **69,2** | **79,8** | **80,1** | **65,2** | **52,3** |
| **Tasso Interno di Rendimento di progetto, lordo imposte** | 7,7% | | | | | | | | | | | | | | |
| Imposte sul reddito di esercizio | - | - | - | - | - | (0,7) | (2,3) | (6,7) | (8,8) | (12,4) | (15,5) | (16,8) | (14,1) | (10,2) | - |
| **Totale flussi di cassa, netto imposte** | - | **(109,7)** | **(49,7)** | **(50,5)** | **(81,5)** | **25,8** | **15,4** | **36,9** | **22,3** | **41,8** | **53,7** | **63,0** | **66,0** | **55,0** | **52,3** |
| **Tasso Interno di Rendimento di progetto, netto imposte** | 5,1% | | | | | | | | | | | | | | |
| **DSCR** | | n.a. | n.a. | n.a. | n.a. | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 1,40 | 2,80 | n.a. | n.a. |
| Finanziamento Outstanding BoP | | 128,9 | 157,7 | 185,0 | 230,7 | 222,5 | 207,1 | 184,3 | 159,7 | 124,7 | 79,2 | 32,2 | 7,2 | - | - |
| **DSCR medio ponderato** | 1,41x | | | | | | | | | | | | | | |
| DSCR minimo | 1,40 | | | | | | | | | | | | | | |

Fonte: PEF, Indici.

45. Altri indicatori che possono essere considerati ai fini della valutazione economico-finanziaria del progetto, ma che non concorrono alla definizione dell'equilibrio economico-finanziario sono i seguenti:

    a. **Il LLCR (Loan Life Coverage Ratio)**, pari al rapporto, periodo per periodo, tra il valore attuale dei flussi di cassa futuri a servizio del debito e il valore del debito.

    b. **Il TIR per gli azionisti,** calcolato come il tasso che rende uguale a zero il valore attuale netto dei flussi di cassa di pertinenza degli azionisti

    c. **Il VAN di progetto,** calcolato attualizzando i flussi di cassa operativi futuri ad un WACC stimato sulla base dei dati di mercato di società ritenute comparabili e della struttura finanziaria target del progetto in questione.

    d. **Il VAN per gli azionisti,** calcolato attualizzando i flussi di cassa agli azionisti ad un costo del capitale di rischio stimato sulla base dei dati di mercato di società ritenute comparabili e della struttura finanziaria target del progetto in questione.

Di seguito si riportano gli indicatori sopra descritti per il progetto in questione (i dati sono in milioni di Euro).

| Indicatori di Equilibrio economico-finanziario | | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Debito Outstanding Inizio Periodo | | 128,9 | 157,7 | 185,0 | 230,7 | 222,5 | 207,1 | 184,3 | 159,7 | 124,7 | 79,2 | 32,2 | 7,2 | - | - |
| Interessi di periodo | | 3,1 | 5,0 | 6,0 | 6,7 | 7,9 | 7,9 | 7,9 | 7,6 | 7,3 | 6,3 | 4,8 | 3,2 | 2,3 | 0,6 |
| Costo Medio del Debito di periodo | | 3,4% | 3,5% | 3,5% | 3,6% | 3,6% | 3,6% | 3,6% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% | 3,7% |
| Flusso di Cassa Disponibile per Rimborso del Debito | | (18,5) | (9,5) | (8,9) | (13,4) | 14,2 | 24,1 | 34,2 | 36,1 | 50,0 | 63,1 | 63,0 | 59,1 | 45,4 | 16,4 |
| Flussi di Cassa Attualizzati | | n.a. | n.a. | n.a. | n.a. | 329,7 | 326,9 | 314,2 | 291,2 | 265,6 | 225,3 | 170,6 | 113,9 | n.a. | n.a. |
| **LLCR** | | n.a. | n.a. | n.a. | n.a. | 1,48 | 1,58 | 1,70 | 1,82 | 2,13 | 2,85 | 5,30 | 15,79 | n.a. | n.a. |
| **LLCR medio ponderato** | **2,00x** | | | | | | | | | | | | | | |
| **LLCR minimo** | **1,48** | | | | | | | | | | | | | | |

| Indicatori di Equilibrio economico-finanziario | | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Apporto azionisti | | (29,0) | (28,3) | (22,8) | (25,1) | - | - | - | (0,0) | - | - | - | - | - | - |
| Dividendi, Rimborso riserva versamento soci, Utili portati a nuovo | | - | - | - | - | 13,0 | - | 10,9 | 16,0 | 9,6 | 18,0 | 18,0 | 60,5 | 43,1 | 15,8 |
| Patrimonio netto fine concessione | | | | | | | | | | | | | | | 1,8 |
| Flussi all'azionista | | (29,0) | (28,3) | (22,8) | (25,1) | 13,0 | - | 10,9 | 16,0 | 9,6 | 18,0 | 18,0 | 60,5 | 43,1 | 17,5 |
| **TIR dell'Azionista** | **8,4%** | | | | | | | | | | | | | | |

| Indicatori di Equilibrio economico-finanziario | | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Flussi di cassa operativi | | (109,7) | (49,7) | (50,5) | (81,5) | 25,8 | 15,4 | 36,9 | 22,3 | 41,8 | 53,7 | 63,0 | 66,0 | 55,0 | 52,3 |
| WACC | **5,2%** | | | | | | | | | | | | | | |
| fattore di sconto | | 1,0 | 0,9 | 0,9 | 0,8 | 0,8 | 0,7 | 0,7 | 0,7 | 0,6 | 0,6 | 0,6 | 0,5 | 0,5 | 0,5 |
| **VAN di progetto** | **(2,5)** | | | | | | | | | | | | | | |

| Indicatori di Equilibrio economico-finanziario | | Anno 0 | Anno 1 | Anno 2 | Anno 3 | Anno 4 | Anno 5 | Anno 6 | Anno 7 | Anno 8 | Anno 9 | Anno 10 | Anno 11 | Anno 12 | Anno 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Flussi di cassa operativi | | (29,0) | (28,3) | (22,8) | (25,1) | 13,0 | - | 10,9 | 16,0 | 9,6 | 18,0 | 18,0 | 60,5 | 43,1 | 17,5 |
| Ke | **9,3%** | | | | | | | | | | | | | | |
| fattore di sconto | | 0,9 | 0,8 | 0,8 | 0,7 | 0,6 | 0,6 | 0,5 | 0,5 | 0,5 | 0,4 | 0,4 | 0,3 | 0,3 | 0,3 |
| **VAN azionisti** | **(5,1)** | | | | | | | | | | | | | | |

46. Di seguito si riporta il calcolo dei tassi di sconto utilizzati per la determinazione del VAN di progetto e per il VAN per gli azionisti. Tali tassi sono stati calcolati sulla base di:

    a. Tasso risk free pari alla media a 10 anni dei titoli governativi italiani (BTP).

    b. Equity market risk premium determinato sulla base di studi specialistici volti a determinare il premio al rischio aggiuntivo che l'investitore dovrebbe richiedere per investire nel mercato azionario rispetto ad uno strumento privo di rischio.

    c. Beta unlevered calcolato sulla base di un panel di società quotate comparabili.

    d. Struttura del debito target del progetto

    e. Costo del debito medio del progetto in relazione alla linea di debito Senior

| **WACC** | |
|---|---|
| Risk-free rate | 0,9% |
| Equity market risk premium | 6,2% |
| Beta Unlevered | 0,51 |
| D/E | 1,65 |
| Beta Levered | 1,35 |
| Market Risk Premium | 8,4% |
| **Ke** | **9,3%** |
| Gross cost of debt | 3,6% |
| Corporate tax rate | 24,0% |
| Tax shield @ 0,0% | (0,9)% |
| **Kd after-tax** | **2,8%** |
| D/(D+E) | 62,2% |
| E/(D+E) | 37,8% |
| **WACC** | **5,2%** |

# XI. Analisi dei Rischi

47. Il Progetto del PSN sarà soggetto a rischi di costruzione, operativi, finanziari, e normativo-regolamentari in carico al concedente e/o al concessionario. La seguente tabella riporta la matrice dei rischi in cui sono descritte le diverse tipologie di rischio per eventi che possono verificarsi durante l'arco temporale della concessione definendone la ripartizione tra concedente e concessionario.

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di progettazione e predisposizione e allestimento** | Rischio derivante da errori od omissioni di progettazione, predisposizione ed allestimento dei locali attrezzati funzionali alla fornitura dei servizi, in relazione alle variabili tecnologiche ed operative | Alta | Ritardi nell'avvio della fase operativa del progetto e/o Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di "costruzione" con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5; Art. 6; Art. 9, comma 1, lett. f); Art. 11; Art. 14; Art. 19; Art. 21; Art. 22; Art. 26; Art. 27; Art. 33, comma 2, lett. a) e c); Art. 39.** |
| **Rischio di domanda** | Rischio di domanda relativo al numero di Amministrazioni utenti che decideranno di migrare nonché alla quantità e tipologia di servizi che le stesse richiederanno | Alta | Diminuzione dei ricavi e dei costi parametrati ai volumi. Contestuale riduzione del MOL, dell'utile netto e del TIR. | Obbligo per le PA di rimborsare il PSN dei i costi sostenuti ed eventualmente corrispondere una fee a parziale copertura dei mancati ricavi In caso di early termination. Riequilibrio del PEF in caso di rendimento inferiori alla soglia individuata. | ✔ | ✔ | **Art. 5; Art. 9, comma 1, lett. a); Art. 10, Art. 11.** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Rischio di Gestione** | Rischio dei ricavi derivante da una errata valutazione delle tariffe applicate | Bassa | Diminuzione dei ricavi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5; Art. 9, comma 1, lett. c); Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 26; Art. 33, comma 2, lett. a), c); Art. 39.** |
| **Rischio di Gestione** | Incremento dei costi di fornitura dei servizi affidati al concessionario | Alta | Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5; Art. 9, comma 1, lett. c); Art. 11; Art. 14; Art. 19; Art. 20; Art. 26 Art. 33, comma 2, lett. a), c); Art. 39.** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Rischi di investimento** | Rischi di investimento legati all'approvvigionamento e ai costi delle componenti degli impianti tecnologici infrastrutturali dei data center funzionali alla fornitura del servizio | Alta | Aumento dei capex e dell'ammortamento relativo, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di approvvigionamento standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5; Art. 9, comma 1, lett. d); Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 33, comma 2, lett. c).** |
| **Rischio di disponibilità** | Rischio di aumento dei costi di manutenzione ordinaria e di manutenzione straordinaria non preventivata o maggiore rispetto a quanto previsto nel PEF | Alta | Aumento dei costi operativi, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5; Art. 9, comma 1, lett. b); Art. 10; Art. 11; Art. 14; Art. 19; Art. 20; Art. 22; Art. 39.** |
| **Rischio di disponibilità** | Mancato rispetto degli standard prestazionali - sia qualitativi che quantitativi - rilevato attraverso gli organismi e meccanismi preposti al controllo, con applicazioni di penali differenziate in ragione del servizio e dell'entità della violazione | Bassa | Aumento dei costi straordinari relativi alle penali, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti con definizioni di penali e rimborsi limitati a un tetto massimo standard. | | ✔ | **Art. 5; Art. 9, comma 1, lett. b); Art. 10; Art. 11; Art. 14; Art. 19; Art. 20; Art. 22;** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | **Art. 23;**<br>**Art. 39.** |
| **Rischi finanziari** | Rischi finanziari relativi al mancato reperimento delle risorse di finanziamento a copertura dei costi e nei tempi prestabiliti e all'oscillazione dei tassi di interesse | Bassa | Potenziale aumento degli oneri finanziari con contestuale diminuzione dell'utile netto e del TIR. | | | ✔ | **Art. 9, comma 1, lett. e);**<br>**Art. 28**<br>**Art. 32** |
| **Forza Maggiore** | Forza maggiore che comporti modifica del Piano Economico-Finanziario. | Minima | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✔ | ✔ | **Art. 11;**<br>**Art. 19;**<br>**Art. 37.** |
| **Mutamenti imposti ex lege** | Mutamenti imposti ex lege (ivi compresi mutamenti relativi ad innovazioni tecnologiche, strumenti e/o tecniche diverse) che comportino modifica del PEF | Media | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✔ | ✔ | **Art. 5;**<br>**Art. 11;**<br>**Art. 37.** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Mutamenti richiesti dal Concedente** | Mutamenti richiesti dal Concedente (es. relativi ad innovazioni tecnologiche) | Molto alta | Riallineamento del PEF. | | ✔ | | **Art. 5; Art. 11; Art. 37** |
| **Danni subiti dal Concedente e da terzi** | Danni subiti dal Concedente e da terzi riconducibili all'espletamento dei servizi, e per tutta la durata della concessione (ex art. 1891) | Bassa | Aumento dei costi straordinari per eventuali rimborsi del danno. | Contratti con clausole limite in caso di rimborso del danno. | | ✔ | **Art. 27 Art. 33, comma 2, lett. d)** |
| **Rischio di valore residuo al termine della Concessione** | Rischio di cessione dei beni non ancora ammortizzati | MEDIA | Rimborso per la devoluzione pari al 90% del valore residuo dell'infrastruttura | | | ✔ | **Art. 38** |
| **Rischio Normativo** | Rispetto del Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione", adottato | Media | Aumento costi | | | ✔ | **Art. 14, comma 9** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | dall'AgID – con Determinazione n. 628/2021 del 15 dicembre 2021 - in conformità alle previsioni di cui all'articolo 33-septies, comma 4, del D.L. 179/2012 e all'articolo 17, comma 6, del D.L. 82/202, e nel rispetto degli atti esecutivi dello stesso Regolamento adottati dall'Agenzia per la cybersicurezza nazionale, d'intesa con il Dipartimento per la trasformazione digitale | | | | | | |

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO G

## MATRICE DEI RISCHI

## Premessa

1. Il Progetto del Polo Strategico Nazionale proposto dal Proponente sarà soggetto ai seguenti rischi:

    - rischio di progettazione e predisposizione e allestimento
    - rischio di domanda
    - rischio di gestione
    - rischio di investimento
    - rischio di disponibilità
    - rischi finanziari
    - forza maggiore
    - mutamenti imposti ex-lege
    - mutamenti richiesti dal Concedente
    - Danni subiti dal Concedente e da terzi

    La seguente tabella riporta la matrice dei rischi in cui sono descritte le diverse tipologie di rischio per eventi che possono verificarsi durante l'arco temporale della concessione definendone la ripartizione tra concedente e concessionario.

    Il presente "Allegato G" " matrice dei rischi", derivante dal modello allegato alla documentazione di gara, è stato integrato sulla base di quanto offerto dal RTI aggiudicatario originario e contenuto nell'offerta tecnica dell'RTI, con Fastweb S.p.a. mandataria, nel documento Annesso 1 all'Allegato B: "Relazione tecnica illustrativa" pagine 75 - 81 contenenti la matrice dei rischi emergente dall'offerta di gara.

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di progettazione e predisposizione e allestimento** | Rischio derivante da errori od omissioni di progettazione, predisposizione ed allestimento dei locali attrezzati funzionali alla fornitura dei servizi, in relazione alle variabili tecnologiche ed operative | Alta | Ritardi nell'avvio della fase operativa del progetto e/o Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR.<br>RISCHIO AUMENTATO IN VIRTU' DEL TERMINE INFERIORE OFFERTO DI 120 GIORNI (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID. CRITERIO 10) | Contratti di "costruzione" con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5;**<br>**Art. 6;**<br>**Art. 9, comma 1, lett. f);**<br>**Art. 11;**<br>**Art. 14;**<br>**Art. 19;**<br>**Art. 21;**<br>**Art. 22;**<br>**Art. 26;**<br>**Art. 27;**<br>**Art. 33, comma 2, lett. a) e c);**<br>**Art. 39.** |
| **Rischio di domanda** | Rischio di domanda relativo al numero di Amministrazioni utenti che decideranno di migrare nonché alla quantità e tipologia di servizi che le stesse richiederanno | Alta | Diminuzione dei ricavi e dei costi parametrati ai volumi. Contestuale riduzione del MOL, dell'utile netto e del TIR. | Obbligo per le PA di rimborsare il PSN dei i costi sostenuti ed eventualmente corrispondere una fee a parziale copertura dei mancati ricavi In caso di early termination. Riequilibrio del PEF in caso di rendimento inferiori alla soglia individuata.<br>SOGLIA DEL TIR DI | ✔ | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. a);**<br>**Art. 10;**<br>**Art. 11.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | | | | PROGETTO RIDOTTA AL 2,2% NEL CASO DI CUI ALL'ART. 11, COMMA 5, (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID CRITERIO 16 | | | |
| **Rischio di gestione** | Rischio dei ricavi derivante da una errata valutazione delle tariffe applicate | Bassa | Diminuzione dei ricavi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche.<br>RISCHIO AUMENTATO IN VIRTU' DEL MECCANISMO DI SCONTO GARANTITO PER LA REVISIONE DEI PREZZI EX ART. 5, COMMA 4, PUNTO iii DELLA BOZZA DI CONVENZIONE (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID. CRITERIO 18) | | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. c);**<br>**Art. 11;**<br>**Art. 14;**<br>**Art. 19;**<br>**Art. 20;**<br>**Art. 22;**<br>**Art. 26;**<br>**Art. 33, comma 2, lett. a), c);**<br>**Art. 39.** |
| **Rischio di Gestione** | Incremento dei costi di fornitura dei servizi affidati al concessionario | Alta | Aumento dei costi operativi con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. c);**<br>**Art. 11;**<br>**Art. 14;**<br>**Art. 19;**<br>**Art. 20;** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | | | | | | | **Art. 26**<br>**Art. 33, comma 2, lett. a), c);**<br>**Art. 39.** |
| **Rischi di investimento** | Rischi di investimento legati all'approvvigionamento e ai costi delle componenti degli impianti tecnologici infrastrutturali dei data center funzionali alla fornitura del servizio | Alta | Aumento dei capex e dell'ammortamento relativo, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti di approvvigionamento standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. d);**<br>**Art. 11;**<br>**Art. 14;**<br>**Art. 19;**<br>**Art. 20;**<br>**Art. 22;**<br>**Art. 33, comma 2, lett. c).** |
| **Rischio di disponibilità** | Rischio di aumento dei costi di manutenzione ordinaria e di manutenzione straordinaria non preventivata o maggiore rispetto a quanto previsto nel PEF | Alta | Aumento dei costi operativi, con contestuale riduzione del MOL, dell'utile netto e del TIR.<br>RISCHIO AUMENTATO IN VIRTU' DELLE MIGLIORIE APPORTATE IN RELAZIONE AGLI INDICATORI DI QUALITA' IQ11, IQ12, IQ13 E IQ14 (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID. | Contratti di appalto standard con previsione di garanzie contrattuali e clausole tipiche. | | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. b);**<br>**Art. 9;**<br>**Art. 10;**<br>**Art. 12;**<br>**Art. 14;**<br>**Art. 20;**<br>**Art. 21;**<br>**Art. 22;**<br>**Art. 38.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | | | CRITERIO 8) | | | | |
| **Rischio di disponibilità** | Mancato rispetto degli standard prestazionali - sia qualitativi che quantitativi - rilevato attraverso gli organismi e meccanismi preposti al controllo, con applicazioni di penali differenziate in ragione del servizio e dell'entità della violazione | Bassa | Aumento dei costi straordinari relativi alle penali, con contestuale riduzione del MOL, dell'utile netto e del TIR. | Contratti con definizioni di penali e rimborsi limitati a un tetto massimo standard. | | ✔ | **Art. 5;**<br>**Art. 9, comma 1, lett. b);**<br>**Art. 10;**<br>**Art. 11;**<br>**Art. 14;**<br>**Art. 19;**<br>**Art. 20;**<br>**Art. 22;**<br>**Art. 23;**<br>**Art. 39.** |
| **Rischi finanziari** | Rischi finanziari relativi al mancato reperimento delle risorse di finanziamento a copertura dei costi e nei tempi prestabiliti e all'oscillazione dei tassi di interesse | Bassa | Potenziale aumento degli oneri finanziari con contestuale diminuzione dell'utile netto e del TIR.<br>RIFINANZIAMENTO:<br>• ABBASSAMENTO DELLA SOGLIA RILEVANTE DI INCREMENTO DEL RENDIMENTO DEL TIR DI PROGETTO ALL'1,8%;<br>• RIDUZIONE DELLA SOGLIA DI INCREMENTO DEL TIR DELL'EQUITY CHE COSTITUISCE IL | | | ✔ | **Art. 9, comma 1, lett. e);**<br>**Art. 28**<br>**Art. 32** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | | | "BENEFICIO DA RIFINANZIAMENTO ALL'1,8% (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID CRITERIO 16) | | | | |
| **Forza Maggiore** | Forza maggiore che comporti modifica del Piano Economico-Finanziario. | Minima | SOSPENSIONE DEL SERVIZIO FINO A 45 GIORNI SENZA DIRITTO AD ALCUNA PROROGA DELLA DURATA CONTRATTUALE.<br>SOSPENSIONE DEL SERVIZIO SENZA DIRITTO AD ALCUN RIEQUILIBRIO DEL PEF FINO A 45 GIORNI (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID CRITERIO 16)<br>Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | SOLO DOPO 45 GIORNI<br>Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo. Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✔ | | **Art. 11;**<br>**Art. 19;**<br>**Art. 37.** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Mutamenti imposti ex lege** | Mutamenti imposti ex lege (ivi compresi mutamenti relativi ad innovazioni tecnologiche, strumenti e/o tecniche diverse) che comportino modifica del PEF | Media | Riallineamento del PEF e potenziale chiusura della concessione, con eventuale implementazione di un termination payment. | Riallineamento del PEF a un caso Base che preveda un TIR dell'azionista minimo.<br>RISCHIO AUMENTATO IN VIRTU' DELL'INNALZAMENTO DELLA PERCENTUALE DI VARIAZIONE DEL TIR DI PROGETTO CHE FA SCATTARE IL RIEQUILIBRIO ALLO 0,17% (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID CRITERIO 16).<br>Potenziale termination payment a carico del concedente dimensionato in modo da coprire almeno il debito e IRR minimo su equity. | ✔ | ✔ | **Art. 5;**<br>**Art. 11;**<br>**Art. 37.** |
| **Mutamenti richiesti dal Concedente** | Mutamenti richiesti dal Concedente (es. relativi ad innovazioni tecnologiche) | Molto alta | Riallineamento del PEF. | | ✔ | | **Art. 5;**<br>**Art. 11;**<br>**Art. 37** |
| **Danni subiti dal Concedente e da terzi** | Danni subiti dal Concedente e da terzi riconducibili all'espletamento dei servizi, e per tutta la durata della concessione (ex art. 1891) | Bassa | Aumento dei costi straordinari per eventuali rimborsi del danno. | Contratti con clausole limite in caso di rimborso del danno. | | ✔ | **Art. 27**<br>**Art. 33, comma 2, lett. d)** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| **Rischio di valore residuo al termine della Concessione** | RISCHIO DI CESSIONE DEI BENI NON ANCORA AMMORTIZZATI | MEDIA | RIMBORSO PER LA DEVOLUZIONE PARI AL 90% VALORE RESIDUO DELL'INFRASTRUTTURA (CFR. Annesso 1 all'Allegato B: Relazione tecnica illustrativa dell'RTI Fastweb ID CRITERIO 16) | | | ✔ | **Art. 38** |
| **Rischio Normativo** | Rispetto del Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione", adottato dall'AgID – con Determinazione n. 628/2021 del 15 dicembre 2021 - in conformità alle previsioni di cui all'articolo 33-septies, comma 4, del D.L. 179/2012 e all'articolo 17, comma 6, del D.L. 82/202, e nel rispetto degli atti esecutivi dello stesso Regolamento adottati dall'Agenzia per la cybersicurezza nazionale, | MEDIA | Aumento costi | | | ✔ | **Art. 14, comma 9** |

| Tipologia di rischio | Descrizione | Probabilità del verificarsi del rischio | Effetti | Strumenti per la mitigazione | Concedente | Concessionario | Riferimenti Contratto |
|---|---|---|---|---|---|---|---|
| | d'intesa con il Dipartimento per la trasformazione digitale | | | | | | |

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1
dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO H

## INDICATORI DI QUALITÀ

Si riporta nel presente allegato l'elenco dei Service Level Agreement (SLA) proposti per l'erogazione dei servizi oggetto del presente progetto. Per ciascuno dei parametri è stabilito un "Valore di Soglia" ovvero il valore minimo che il costituendo ATI si impegna a garantire
Al superamento del "Valore di Soglia" scatterà il meccanismo di applicazione delle relative penali. Al fine dell'applicazione delle penali saranno considerati i "Valori di Soglia" indicati nel presente documento elaborato a partire dalla documentazione di gara (cfr. Allegato A - Annesso 2 "Specificazione delle caratteristiche del servizio e della gestione") ed opportunamente modificato ed integrato rispetto a quanto indicato nell'offerta risultata economicamente più vantaggiosa (i.e. Allegato B - Annesso 1 "Relazione tecnica illustrativa" dell'RTI Fastweb).

Ai fini del presente documento si intende:

- per "DTD" si intende il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri;
- per "Amministrazione", l'Amministrazione Utente che sottoscrive il Contratto Esecutivo con il Concessionario per usufruire dei relativi servizi oggetto della fornitura.

Di seguito la tabella di riepilogo, che schematizza la matrice di corrispondenza tra gli Indicatori di Qualità validi per l'intera fornitura, l'ambito di applicazione, la presenza di una azione contrattuale previste nel caso di non rispetto (Penale) e il soggetto verso cui sarà tenuta la rendicontazione:

| Ambito | ID | Descrizione | Penale | Rendicontazione |
|---|---|---|---|---|
| Governo della Fornitura | IQ01 | Invio rendicontazione flussi mensili | Sì | DTD |
| | IQ02 | Invio rendicontazione flussi annuali | Sì | DTD |
| | IQ03 | Rispetto di una scadenza temporale | Sì | Amministrazione |
| | IQ04 | Non approvazione di documenti | Sì | Amministrazione |
| | IQ05 | Attivazione degli interventi | Sì | Amministrazione |
| | IQ06 | Disponibilità degli strumenti di supporto | Sì | Amministrazione |
| Erogazione dei Servizi | IQ07 | Indisponibilità Infrastruttura | Sì | DTD |
| | IQ08 | Disponibilità del servizio di Infrastruttura (Housing) | Sì | Amministrazione |
| | IQ09 | Disponibilità del servizio di Infrastruttura (Hosting) | Sì | Amministrazione |
| | IQ010 | Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS | Sì | Amministrazione |
| | IQ011 | Rispetto dell'RTO | Sì | Amministrazione |
| | IQ012 | Rispetto dell'RPO | Sì | Amministrazione |
| | IQ013 | Rispetto dell'RTO (DR su diversa Region) | Sì | Amministrazione |

| | | | | |
|---|---|---|---|---|
| | IQ014 | Rispetto dell'RPO (DR su diversa Region) | Sì | Amministrazione |
| | IQ015 | Disponibilità dei dati a fine fornitura | Sì | Amministrazione |
| Help Desk | IQ016 | Tempo di presa in carico | Sì | Amministrazione |
| | IQ017 | Tempo di risoluzione | Sì | Amministrazione |
| Migrazione | IQ018 | Rispetto dei volumi previsti nel piano di migrazione | Sì | Amministrazione |

Il presente Allegato riporta gli Indicatori di Qualità risultanti all'esito della Gara e costituisce la fonte corretta per la implementazione e verifica degli stessi.

## *1 INDICATORI DI QUALITÁ PER IL GOVERNO DELLA FORNITURA*

| **ID** | **IQ01** | **PARAMETRO** | **Invio rendicontazione flussi mensili** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità verifica il ritardo del Fornitore nel produrre e fornire all'Amministrazione i documenti contrattuali della Convenzione nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati | |
| **FORMULA** | | IQ01 = $data_{eff}$ – $data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Mensile | |
| **VALORE DI SOGLIA** | | IQ01 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il DTD applicherà una penale pari ad € 200,00. | |
| **APPLICAZIONE** | | DTD | |

| **ID** | **IQ02** | **PARAMETRO** | **Invio rendicontazione flussi annuali** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità verifica il ritardo del Fornitore nel produrre e fornire all'Amministrazione i documenti contrattuali della Convenzione nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati | |
| **FORMULA** | | IQ02 = $data_{eff}$ – $data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Annuale | |
| **VALORE DI SOGLIA** | | IQ02 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il DTD applicherà una penale pari ad € 500,00. | |
| **APPLICAZIONE** | | DTD | |

| **ID** | **IQ03** | **PARAMETRO** | **Rispetto di una scadenza temporale** |
|---|---|---|---|

| | |
|---|---|
| **DESCRIZIONE** | Per ciascun servizio e per ciascun deliverable prodotto nell'ambito dello stesso, il rispetto di una scadenza stabilita dal contratto e/o indicata nel Progetto di fattibilità |
| **FORMULA** | IQ03 = $data_{eff}$ – $data_{prev}$<br>Data prevista di consegna di un deliverable (data_prev)<br>Data effettiva di consegna di un delivarable (data_eff) |
| **FREQUENZA DI MISURAZIONE** | A EVENTO |
| **VALORE DI SOGLIA** | IQ03 ≤ 0 |
| **PENALE** | Per ogni giorno lavorativo eccedente la soglia, l'Amministrazione applicherà la penale pari allo 0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale dell'obiettivo/servizio di riferimento nel contratto esecutivo di fornitura. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ04** | **PARAMETRO** | **Non approvazione di documenti** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore si applica alla mancata approvazione di un documento basilare per le attività progettuali. Sono inderogabilmente basilari i seguenti documenti:<br>• deliverable di fornitura<br>• il Piano di lavoro generale<br>• I verbali di stato di avanzamento lavori – SAL.<br>Nel corso della fornitura l'Amministrazione potrà indicare ulteriori documenti.<br>La fonte dei dati possono essere E-mail, lettere, verbali.<br>Viene definito il parametro "N_rilievi" che verrà incrementato di una unità ogniqualvolta un documento non verrà approvato | |
| **FORMULA** | | IQ04 = N_rilievi<br>Nr di documenti (deliverables) non approvati = N_rilievi + 1 | |
| **FREQUENZA DI MISURAZIONE** | | A semestre | |
| **VALORE DI SOGLIA** | | IQ04 < 0 | |
| **PENALE** | | Il superamento del valore soglia comporterà per ogni documento aggiuntivo rispetto al valore soglia l'applicazione della penale "Non approvazione di documenti" pari a 500€. | |
| **APPLICAZIONE** | | Amministrazione | |

| ID | IQ05 | PARAMETRO | Attivazione degli interventi |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore misura la tempestività di attivazione degli interventi relativi ai servizi professionali a partire dalla richiesta dell'Amministrazione.<br>Viene misurato in giorni lavorativi. | |
| **FORMULA** | | *IQ05 = Data_attiv_int - Data_rich_int*<br>dove per ciascun intervento vanno rilevati - Data della richiesta di attivazione di un intervento (Data_rich_int) - Data di attivazione dell'intervento (Data_attiv_int) | |
| **FREQUENZA DI MISURAZIONE** | | A EVENTO | |
| **VALORE DI SOGLIA** | | Per interventi pianificati nel Piano di Lavoro Generale: IQ05 = 0 negli altri casi: IQ05 <= 5 giorni lavorativi | |
| **PENALE** | | Per ogni 5 giorni lavorativi o frazione eccedenti il valore di soglia l'Amministrazione applicherà la penale "Ritardo nell'attivazione dell'intervento" pari all'1‰ dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura | |
| **APPLICAZIONE** | | Amministrazione | |

| ID | IQ06 | PARAMETRO | Disponibilità degli strumenti di supporto |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura la disponibilità degli strumenti di supporto messi a disposizione dell'Amministrazione di seguito elencati, resi disponibili dal costituendo ATI per l'erogazione dei servizi stessi per l'intera durata contrattuale:<br>● Portale di Governo e Gestione della Fornitura;<br>● Cruscotto sintetico di controllo/monitoraggio della fornitura;<br>● Sistema di Trouble Ticketing;<br>● Sistema di gestione documentale.<br>Il servizio erogato dagli strumenti di supporto si intende indisponibile quando esso viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso del costituendo ATI e della connettività, mancato funzionamento dell'impianto antincendio e di condizionamento, problematiche IT della piattaforma Host, problematiche IT relative al middleware e applicative che inibiscono la completa fruizione del servizio.<br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio erogato dai sistemi di supporto è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |

| | | |
|---|---|---|
| **FORMULA** | Si definisce “disponibilità” del servizio, espressa come valore percentuale:<br>IQ06 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell’ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br>T = 24x60x365-FMM | |
| **FREQUENZA DI MISURAZIONE** | Annuale | |
| **VALORE DI SOGLIA** | Soglia minima; IQ06 ≥ 99,70% | |
| **PENALE** | L’indisponibilità della infrastruttura a supporto della erogazione dei servizi per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l’emissione di una penale pari al 1‰ (uno per mille) dell’importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. | |
| **APPLICAZIONE** | Amministrazione | |

## *2 INDICATORI DI QUALITÁ PER L'EROGAZIONE DEI SERVIZI*

| **ID** | **IQ07** | **PARAMETRO** | **Indisponibilità Infrastruttura** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore di qualità rappresenta il rispetto della scadenza di messa in esercizio dell'Infrastruttura proposta dal fornitore nei tempi previsti, ossia entro 4 mesi (120 giorni) dalla stipula del contratto. | |
| **FORMULA** | | IQ07 = $data_{eff} - data_{prev}$<br>Data prevista di avvio attività (data_prev)<br>Data effettiva di avvio attività (data_eff) | |
| **FREQUENZA DI MISURAZIONE** | | Ad evento | |
| **VALORE DI SOGLIA** | | IQ07 ≤ 0 | |
| **PENALE** | | Per ogni giorno lavorativo eccedente la soglia il DTD applicherà una penale pari ad € 150.000. | |
| **APPLICAZIONE** | | DTD | |

| **ID** | **IQ08** | **PARAMETRO** | **Disponibilità del servizio di Infrastruttura (Housing)** |
|---|---|---|---|
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità Housing) si intende indisponibile quando l'esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso del costituendo ATI e della connettività, il mancato funzionamento dell'impianto antincendio e di condizionamento e qualunque evento riconducibile alla responsabilità del costituendo ATI.<br>L'indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |

| | |
|---|---|
| **FORMULA** | Si definisce “disponibilità” del servizio, espressa come valore percentuale:<br>IQ08 = (1 – $\frac{\sum_{j=1}^{M} d_j}{T}$ ) x 100<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell’ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre di Manutenzione Programmata e straordinaria Impianti Data Center (MPSIDC).<br>T = 24x60x365-MPSIDC |
| **FREQUENZA DI MISURAZIONE** | Annuale |
| **VALORE DI SOGLIA** | Soglia minima; IQ08 ≥ 99,980% |
| **PENALE** | L’indisponibilità servizi infrastrutturali di Housing per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l’emissione di una penale pari al 1‰ (uno per mille) dell’importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ09** | **PARAMETRO** | **Disponibilità del servizio di Infrastruttura (Hosting)** |
|---|---|---|---|
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità Hosting) si intende indisponibile quando l’esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso del costituendo ATI e della connettività, mancato funzionamento dell’impianto antincendio e di condizionamento, problematiche IT della piattaforma Host e qualunque altro evento riconducibile alla responsabilità del costituendo ATI.<br>L’indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |

| | |
|---|---|
| **FORMULA** | Si definisce “disponibilità” del servizio, espressa come valore percentuale:<br>IQ09 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell’ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br>T = 24x60x365-FMM |
| **FREQUENZA DI MISURAZIONE** | Annuale |
| **VALORE DI SOGLIA** | Soglia minima: IQ09 ≥ 99.95% |
| **PENALE** | L’indisponibilità della infrastruttura a supporto della erogazione dei servizi di Hosting per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l’emissione di una penale pari al 1‰ (uno per mille) dell’importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. |
| **APPLICAZIONE** | Amministrazione |

| **ID** | **IQ010** | **PARAMETRO** | **Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS** |
|---|---|---|---|
| **DESCRIZIONE** | | Il servizio di Infrastruttura (in modalità IaaS, PaaS, BaaS, CaaS) si intende indisponibile quando l’esercizio del servizio erogato viene compromesso a causa di: mancata continuità elettrica, indisponibilità della rete di accesso del costituendo ATI e della connettività, mancato funzionamento dell’impianto antincendio e di condizionamento, problematiche IT della piattaforma Host e qualunque altro evento riconducibile alla responsabilità del costituendo ATI.<br>L’indicatore di qualità rappresenta la percentuale di tempo durante il quale il servizio è funzionante rispetto al periodo di osservazione contrattuale, in funzione della finestra temporale di erogazione detratte le finestre mensili di manutenzione.<br>Eventuali interruzioni di servizio necessarie alla corretta esecuzione delle attività di commisioning e decomissioning, purché precedentemente comunicate, non saranno conteggiate. | |

| | | | |
|---|---|---|---|
| **FORMULA** | Si definisce “disponibilità” del servizio, espressa come valore percentuale:<br>IQ010 = ( 1 – $\frac{\sum_{J=1}^{M} d_j}{T}$ ) x 100<br>Dove:<br>M = numero totale di disservizi;<br>dj = durata, espressa in minuti, del disservizio j-esimo nell’ambito della finestra temporale di erogazione;<br>T = finestra temporale di misurazione della disponibilità pari al tempo totale espresso in minuti della finestra temporale di erogazione del servizio nel periodo di osservazione contrattuale (pari a 12 mesi) detratte le finestre mensili di manutenzione (FMM).<br>T = 24x60x365-FMM | | |
| **TEMPO MISURAZIONE SLA** | Annuale | | |
| **VALORE DI SOGLIA** | Soglia minima: IQ010 ≥ 99.95% | | |
| **PENALE** | L’indisponibilità della infrastruttura IaaS, PaaS, BaaS, CaaS per un tempo complessivo superiore o uguale al valore soglia richiesto costituisce disservizio e comporta l’emissione di una penale pari al 1‰ (uno per mille) dell’importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. | | |
| **APPLICAZIONE** | Amministrazione | | |
| **ID** | **IQ011** | **PARAMETRO** | **Rispetto dell’RTO** |
| **DESCRIZIONE** | Il presente indicatore di qualità misura il rispetto del RTO (Recovery Time Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al costituendo ATI. Il valore target è 30 minuti. | | |
| **FORMULA** | IQ011 = (RTO_effettivo - RTO_atteso)<br>dove RTO_atteso = 5 minuti | | |
| **FREQUENZA DI MISURAZIONE** | Ad evento | | |
| **VALORE DI SOGLIA** | Soglia minima: IQ011 <= 0 | | |
| **PENALI** | Per ogni minuto eccedente la soglia, l’Amministrazione applicherà la penale pari all’0,1‰ (zerovirgolauno per mille) dell’importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | | |
| **APPLICAZIONE** | Amministrazione | | |

| | | | |
|---|---|---|---|
| **ID** | **IQ012** | **PARAMETRO** | **Rispetto dell’RPO** |

| | |
|---|---|
| **DESCRIZIONE** | Il presente indicatore di qualità misura il rispetto del RPO (Recovery Point Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al Fornitore.<br>Valore di RPO rappresenta la perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario.<br>Il valore target è 15 secondi. |
| **FORMULA** | IQ012 = $\frac{N_C - N_{CFuoriSoglia}}{N_C}$ x 100<br>dove:<br>$N_C$ = Numero di campionamenti = 104 (2 campionamenti a settimana)<br>$N_{CFuoriSoglia}$ = Numero dei campioni per cui il valore si discosta dal valore soglia |
| **FREQUENZA DI MISURAZIONE** | Campionamento effettuato due volte a settimana.<br>SLA su base annuale |
| **VALORE DI SOGLIA** | Soglia minima: IQ012 ≥ 99% |
| **PENALI** | Per ogni 1% (uno per cento) di scostamento dalla soglia definita, nonché per ogni<br>caso di verificata inconsistenza dei dati di replica, l'Amministrazione applicherà<br>una penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. |
| **APPLICAZIONE** | Amministrazione |

| | | | |
|---|---|---|---|
| **ID** | **IQ013** | **PARAMETRO** | **Rispetto dell'RTO su diversa Region** |
| **DESCRIZIONE** | | Il presente indicatore di qualità misura il rispetto del RTO (Recovery Time Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al costituendo ATI. Il valore target è 4 ore. | |
| **FORMULA** | | IQ013 = (RTO_effettivo - RTO_atteso)<br>dove RTO_atteso = 25 minuti | |
| **FREQUENZA DI MISURAZIONE** | | Ad evento | |
| **VALORE DI SOGLIA** | | Soglia minima; IQ013 ≤ 0 | |
| **PENALI** | | Per ogni ora solare eccedente la soglia, l'Amministrazione applicherà la penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | | Amministrazione | |

| ID | IQ014 | PARAMETRO | Rispetto dell'RPO su diversa Region |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità misura il rispetto del RPO (Recovery Point Objective) nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al Fornitore.<br>Valore di RPO rappresenta la perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario.<br>Il valore target è 10 minuti | |
| **FORMULA** | | IQ014 = $\frac{N_C - N_{CFuoriSoglia}}{N_C}$ x 100<br>dove:<br>$N_C$ = Numero di campionamenti = 104 (2 campionamenti a settimana)<br>$N_{CFuoriSoglia}$ = Numero dei campioni per cui il valore si discosta dal valore soglia | |
| **FREQUENZA DI MISURAZIONE** | | Campionamento effettuato due volte a settimana.<br>SLA su base annuale. | |
| **VALORE DI SOGLIA** | | Soglia minima; IQ014 ≥ 99% | |
| **PENALI** | | Per ogni 1% (uno per cento) di scostamento dalla soglia definita, nonché per ogni<br>caso di verificata inconsistenza dei dati di replica, l'Amministrazione applicherà<br>una penale pari all'1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | | Amministrazione | |

| ID | IQ15 | PARAMETRO | Disponibilità dei dati a fine fornitura |
|---|---|---|---|
| **DESCRIZIONE** | | Il presente indicatore di qualità monitora il rispetto della scadenza di consegna/riconsegna dei principali deliverable e oggetti della fornitura (es. almeno i dati memorizzati nei DB, file di configurazione, immagine server etc …) stabilita dal contratto e/o dal piano di lavoro approvato, con indicazione della data di fine fornitura.<br>In particolare, l'indicatore riguarda la disponibilità verso l'Amministrazione dei dati conservati/configurazioni nell'ambito dei Centri Servizi alla fine della fornitura della singola componente di servizio. | |
| **FORMULA** | | IQ15 = data_eff - data_ prev<br>dove:<br>data_prev = Data prevista di consegna/riconsegna (concordata con l'Amministrazione)<br>data_eff = Data effettiva di consegna/riconsegna | |

| | | |
|---|---|---|
| **FREQUENZA DI MISURAZIONE** | A Evento | |
| **VALORE DI SOGLIA** | Soglia minima: IQ015 ≤ 0 | |
| **PENALI** | Per ogni giorno lavorativo eccedente la soglia, l'Amministrazione contraente applicherà la penale pari all'0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura. | |
| **APPLICAZIONE** | Amministrazione | |

## *3 INDICATORI DI QUALITÁ PER L'HELP DESK*

| **ID** | **IQ016** | **PARAMETRO** | **Tempo di presa in carico** |
|---|---|---|---|
| **DESCRIZIONE** | | Tempestività di presa in carico delle richieste multicanale ricevute da parte dell'Help Desk e relative ad anomalie e/o richiesta di accesso al Data Center.<br>Tempo, misurato in minuti, intercorrente tra la richiesta e la presa in carico della stessa coincidente con l'apertura del ticket da parte dell'help desk.<br>Il periodo di riferimento per la rilevazione dell'indicatore è pari a 3 mesi.<br>Il valore target è 10 minuti | |
| **FORMULA** | | IQ016= $\frac{N_{richiesta_{presaincarico}(T_{presaincarico} \leq 10\ min)}}{N_{richieste}}$ x 100<br>Dove:<br>T_presaincarico = Data_presaincarico_ric – Data_invio_ric<br>Data_invio_ric = Data ora (hh/mm/ss) dell'invio della richiesta<br>Data_presaincarico_ric = Data ora (hh/mm/ss) della effettiva presa in carico della richiesta<br>Numero di richiesta prese in carico (N_richiesta_presaincarico)<br>Numero totale di richieste (N_richieste) | |
| **FREQUENZA DI MISURAZIONE** | | Trimestrale | |
| **VALORE DI SOGLIA** | | Soglia minima: IQ016 ≥ 97,00% | |
| **PENALI** | | Il mancato raggiungimento del valore di soglia comporterà l'applicazione della penale pari allo 0,5‰ (zerovirgolacinque per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura, per ogni punto percentuale in diminuzione rispetto al valore soglia. | |

Relativamente all'indicatore di qualità "**Tempo di risoluzione**", è importante introdurre il concetto di "priorità" come elemento qualificante il problema. Di seguito la classificazione:

- **Priorità 1**: problema di tipo bloccante, per cui è impedito agli utenti l'utilizzo dei servizi ed alle eventuali componenti funzionali dei singoli servizi;
- **Priorità 2**: problema per cui è impedito agli utenti l'utilizzo di una funzione del servizio in alcune specifiche condizioni (ad esempio per alcuni dati di input);
- **Priorità 3**: richiesta di tipo informativo per cui risulta difficoltoso per gli utenti l'utilizzo di una funzione del servizio o sono necessarie ulteriori informazioni (o materiale documentale a supporto) o richiese relative a problematiche amministrative/contrattuali.

La seguente tabella indica i tempi massimi di risoluzione in funzione della priorità attribuita al problema.

| Priorità del problema | T_max - Tempo massimo di risoluzione (ore lavorative) |
|---|---|
| Priorità 1 | ≤ 2 ore |
| Priorità 2 | ≤ 4 ore |
| Priorità 3 | ≤ 6 ore |

Di seguito il dettaglio dell'indicatore:

| **ID** | **IQ017** | **PARAMETRO** | **Tempo di risoluzione** |
|---|---|---|---|
| **DESCRIZIONE** | | Tempestività nell'esecuzione delle attività necessarie alla risoluzione delle richieste ricevute tramite il servizio di Help Desk e relative ad anomalie e/o richiesta di informazioni. Sono comprese le richieste aperte in automatico dagli Strumenti di monitoraggio e controllo.<br>Il valore target è differenziato per il livello di priorità attribuito al problema ed è riportato nella tabella precedente; sulla base dei 3 distinti valori target, si differenzieranno 3 diversi indicatori di qualità: IQ017a, IQ017b e IQ017c, definiti sulla base della successiva formulazione. | |
| **FORMULA** | | IQ017a = $\frac{N_{richieste\ (T_{risoluzione} \leq T_{Max_Priorità1})}}{N_{richieste}}$ x 100<br>IQ017b = $\frac{N_{richieste\ (T_{risoluzione} \leq T_{Max_Priorità2})}}{N_{richieste}}$ x 100<br>IQ017c = $\frac{N_{richieste\ (T_{risoluzione} \leq T_{Max_Priorità3})}}{N_{richieste}}$ x 100<br>dove:<br>*T_risoluzione = Data_risol_ric – Data_aper_ric - T_pending*<br>e dove:<br>● *Data_aper_ric* = Data Ora (hh/mm/ss) della effettiva presa in carico;<br>● *Data_riso_ric* = Data Ora (hh/mm/ss) della risoluzione;<br>● *T_pending* = Tempo di pending complessivo;<br>● *N_richieste* = Numero totale di richieste. | |
| **FREQUENZA DI MISURAZIONE** | | Trimestrale | |
| **VALORE DI SOGLIA** | | Soglia minima:<br>IQ017a >= 99%<br>IQ017b >= 97%<br>IQ017c >= 95% | |

| | |
|---|---|
| **PENALI** | Il mancato raggiungimento del valore di soglia comporterà l'applicazione della penale pari allo 1‰ (uno per mille) dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura per ogni punto percentuale in diminuzione rispetto al valore soglia. |

## *4 INDICATORI DI QUALITÁ PER IL SERVIZIO DI MIGRAZIONE*

| **ID** | **IQ018** | **PARAMETRO** | **Rispetto dei volumi previsti nel piano di migrazione** |
|---|---|---|---|
| **DESCRIZIONE** | | L'indicatore misura lo scostamento % tra i workload migrati e quelli previsti dal piano di migrazione concordato tra le parti in fase di progetto.<br>Per tener conto dei ritardi non dovuti al team di migrazione, andrà revisionato in modo coerente lo SLA target dell'anno e il target degli anni successivi. | |
| **FORMULA** | | IQ018 = $\frac{Numero_{workload_{previsti}} - Numero_workload_{migrati}}{Numero_workload_previsti}$ x 100 | |
| **FREQUENZA DI MISURAZIONE** | | Annuale | |
| **VALORE DI SOGLIA** | | Soglia minima:<br>IQ018 ≤ 10,00% per il primo anno<br>IQ018 ≤ 5,00% per gli anni successivi | |
| **PENALI** | | Il superamento del valore di soglia comporterà l'applicazione della penale pari allo 1,5% (unovirgolacinque per cento) dell'importo annuale, per ogni 10 punti percentuali in eccedenza rispetto al valore soglia. | |

# CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

## ALLEGATO I

### FLUSSI INFORMATIVI

INDICE

1 Comunicazione delle informazioni obbligatorie per il monitoraggio della Convenzione 3

1.1 Flussi di monitoraggio mensili 3

1.2 Flussi di monitoraggio annuale 4

**Premessa**

Il presente documento disciplina i termini e le modalità di invio delle principali comunicazioni obbligatorie previste dalla Convenzione. Ulteriori informazioni potranno essere comunque richieste dal MITD.

## *1 Comunicazione delle informazioni obbligatorie per il monitoraggio della Convenzione*

Nell'ambito dell'attività di monitoraggio della Concessione svolta dal DTD, si richiede al Concessionario di comunicare le informazioni obbligatorie all'indirizzo PEC diptrasformazionedigitale@pec.governo.it.

Le informazioni da comunicare devono essere inviate secondo le tempistiche di seguito riportate:

- Flussi di monitoraggio mensili
- Flussi di monitoraggio annuali

I dettagli dei due flussi sono di seguito riportati.

### *1.1 Flussi di monitoraggio mensili*

A partire dalla data di stipula e con cadenza mensile il Concessionario entro il 15 (quindici) del mese successivo di scadenza del flusso dovrà inviare un file in formato XML contenente le seguenti informazioni:

- Contratti di Utenza stipulati:
  - Codice fiscale dell'Amministrazione o Ente Contraente;
  - Codice IPA;
  - Denominazione dell'Amministrazione o Ente Contraente;
  - Importo del Contratto;
  - CIG del Contratto;
  - Data di stipula, indica la data in cui viene stipulato il contratto;
  - Data termine del Contratto o durata;
  - PEC dell'Amministrazione;
  - Contatto riferimento dell'Amministrazione;

### *1.2 Flussi di monitoraggio annuale*

A partire dalla data di stipula e con cadenza annuale il Concessionario entro il 31 gennaio dovrà inviare un file in formato XML contenente le seguenti informazioni che consuntivano le attività svolte nell'anno precedente:

- Contratti di Utenza stipulati:
  - Codice fiscale dell'Amministrazione o Ente Contraente;
  - Codice IPA;
  - Denominazione dell'Amministrazione o Ente Contraente;
  - Importo del Contratto;
  - CIG del Contratto;
  - Data di stipula, indica la data in cui viene stipulato il contratto;
  - Data termine del Contratto o durata;
  - PEC dell'Amministrazione;
  - Contatto riferimento dell'Amministrazione;

- Per ogni Amministrazione aderente:
  - Tipologia e quantità di servizi erogati;
  - Fatturato corrispondente;
  - Eventuali penali maturate;
  - Penali riconosciute;

- Per Famiglia di Servizi:
  - Tipologia e quantità di servizi erogati;
  - Fatturato corrispondente.

Sempre con cadenza annuale il Concessionario entro il 31 maggio dell'anno successivo dovrà trasmettere:

- PEF Consuntivo cumulato a partire dalla data di stipula;
- PEF aggiornato (consuntivo e prospettico);
- Relazione sull'andamento della gestione.

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO K

## DUVRI CONTRATTUALE

**Considerazioni di carattere generale**

In considerazione della natura dei servizi oggetto della presente procedura, non sussiste, ai sensi dell'art. 26 del d.lgs. 9 aprile 2008 n. 81, l'obbligo di procedere alla predisposizione dei documenti di cui all'art. 26 commi 3 e 3 ter del predetto decreto.

Nello specifico tutti i servizi Core verranno erogati presso le sedi del Concessionario, dei soci dello stesso e/o dei propri fornitori dei servizi (i.e. Cloud Services Provider), non ricadendo pertanto negli obblighi di cui sopra. Lo stesso vale per i Servizi no Core in quanto servizi di natura intellettuale.

**Considerazioni di carattere specifico relativo ai Contratti d'utenza**

Fermo restando quanto sopra, in alcuni casi specifici per cui l'erogazione dei servizi no Core preveda l'intervento presso le sedi dell'Amministrazione Utente che richieda l'adozione di specifiche istruzioni per il rispetto della normativa suddetta, ovvero l'Amministrazione Utente richieda taluni servizi opzionali inseriti nel listino (Connettività e Moving server) sarà responsabilità di questa ultima predisporre il DUVRI specifico che dovrà essere messo a disposizione del Concessionario prima dell'erogazione dei servizi medesimi.

CONCESSIONE

per la realizzazione e
gestione di una nuova infrastruttura informatica al servizio della
Pubblica Amministrazione
denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1
dell'articolo 33-septies del
d.l. n. 179 del 2012.

# ALLEGATO L

## ELENCO DEI SERVIZI *CORE*, NO *CORE* E *CSP*

## I servizi Core che saranno erogati dal Concedente sono i seguenti

a. Housing

b. Hosting

c. IaaS Private, IaaS Shared

d. Altri servizi di IaaS e Cloud: Congiuntamente ai servizi principali di IaaS (Private e Shared) il Concedente offrirà alle Amministrazioni utenti una serie di servizi IaaS e Cloud specifici e/o complementari, e in particolare:

   i. Platform as a Service (PaaS)

   ii. Containers-as-a-Service (CaaS)

   iii. Disaster Recovery per IaaS e Cloud

e. Hybrid Cloud on PSN Site

f. Public Cloud PSN Managed

g. Secure Public Cloud

h. PaaS Industry

i. Migrazione

I servizi CSP corrispondono ai servizi Core di cui ai punti e. Hybrid Cloud on PSN Site, f. Public Cloud PSN Managed, g. Secure Public Cloud.

## Viene anche fornito a complemento l'elenco dei Servizi no Core

j. Business & Culture enablement

k. Servizi professionali

l. Replatform e Rearchitect

m. IT infrastructure - service operations