SISTEMA SANITARIO REGIONALE
ASL ROMA 5

REGIONE LAZIO

REGIONE LAZIO
AZIENDA SANITARIA LOCALE ROMA 5

DELIBERAZIONE N° 000331 **DEL** 08 FEB. 2024

STRUTTURA PROPONENTE: UOC I.T.
Oggetto: Piano Nazionale Ripresa e Resilienza (PNRR) – Missione 1 - Componente 1 – Investimento 1.1 "Infrastrutture Digitali" e Investimento 1.2 "Abilitazione al Cloud per le PA Locali" – Adesione ASL Roma 5 alla Convenzione sottoscritta tra PSN S.p.A. e Dipartimento per la Trasformazione Digitale della PCM per la migrazione al PSN – Importo complessivo intervento € 5.121.095,62 - CUP G31C23000840006

PARERE DEL DIRETTORE AMMINISTRATIVO Dott. Filippo Coiro

☒ Favorevole ☐ Non favorevole (vedi motivazioni allegate)

data 08 FEB. 2024

PARERE DEL DIRETTORE SANITARIO *f.f.* Dott. Franco Cortellessa

☒ Favorevole ☐ Non favorevole (vedi motivazioni allegate)

data 08 FEB. 2024

Atto trasmesso al Collegio Sindacale

☐ Senza osservazioni ☐ Con osservazioni (vedi allegato)

Il Presidente _____ data _____

Il Dirigente addetto al controllo del budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico.

Voce del conto economico su cui si imputa la spesa: 502020106-

Registrazione n. 2024/669- del 08/02/2024

Il Dir. UOC Bilancio e Contabilità (Dott. Fabio Filippi _____

Il Dirigente e/o il responsabile del procedimento proponente, con la sottoscrizione del presente atto a seguito dell'istruttoria effettuata attesta che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico

Il Resp.le F.O. Gestione Amm.va e di Progetto Dr.ssa M. Fatima Pellegrino _____

Il Direttore *f.f.* UOC I.T. Dott. Luca Centurelli _____

La presente deliberazione è costituita da n. 6 pagine

Da n. 1 allegati per un totale di n. 196 pagine

Il **Direttore *f. f.* UOC IT** relaziona al Direttore Generale quanto segue e sottopone il seguente schema di deliberazione:

Ai sensi e per gli effetti della Deliberazione n. 933 del 19/07/2019, parzialmente modificata con Deliberazione n.1126 del 10/09/2019, con la quale è stato adottato l'Atto Aziendale pubblicato sul B.U.R.L. n. 84 del 17/10/2019 e della deliberazione n.993 del 07/06/2022 con la quale sono state proposte modifiche all'Atto Aziendale approvate con determina regionale G07864 del 16/06/2022 e pubblicate sul B.U.R.L. n.56, suppl.1, del 05/07/2022;

PREMESSO che il Piano Nazionale di Ripresa e Resilienza (PNRR), trasmesso dal Governo Italiano alla Commissione Europea il 30 aprile 2021 ai sensi degli articoli 18 e seguenti del regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, definisce un quadro di investimenti e riforme a livello nazionale, con corrispondenti obiettivi e traguardi cadenzati temporalmente, al cui conseguimento si lega l'assegnazione di risorse finanziarie messe a disposizione dall'Unione Europea;

VISTI la "Procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico-privato, della realizzazione e gestione del Polo Strategico Nazionale", operata da Difesa Servizi S.p.A. per conto del Dipartimento per la Trasformazione Digitale (di seguito anche DTD) e affidata all'operatore concessionario Polo Strategico Nazionale S.p.A., società partecipata dalle imprese TIM, Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei;

la Convenzione di concessione stipulata, ai sensi degli artt. 164, 165, 179, 180, comma 3, 183, comma 15, del d.lgs. n. 50 del 2016, in data 24 agosto 2022 tra Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – e la società di progetto Polo Strategico Nazionale Spa, con sede legale in Roma, via G. Puccini n.6, Codice Fiscale e Partita IVA 16825251008, per la prestazione da parte del Concessionario in favore delle singole Amministrazioni Utenti, in maniera continuativa e sistematica, di un Catalogo dei 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 amministrazione;

l'avviso pubblico multimisura per la presentazione di domande di partecipazione a valere sul PNRR - Missione 1 - Componente 1 - Investimento 1.1 "Infrastrutture Digitali" e Investimento 1.2 "Abilitazione al cloud per le PA Locali ASL/AO", pubblicato in data 14/03/2023 sulla piattaforma https://padigitale2026.gov.it;

ATTESO che gli investimenti, di cui all'avviso sopra richiamato, sono collegati all'obbligo per la PA di migrare i propri CED verso ambienti Cloud, così come previsto dall'ex art. 35 del D.L. 76/2020 di modifica dell'articolo 33-septies (Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese) del DL 179/2012, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221;

DATO ATTO che in data 11/07/2023 la ASL Roma 5 ha inoltrato la propria candidatura all'avviso di che trattasi sulla piattaforma https://padigitale2026.gov.it, con Codice identificativo della candidatura 86264;

che la suddetta domanda è stata predisposta in ottemperanza rispetto a quanto richiesto dall'amministrazione regionale per la migrazione al Cloud delle Aziende del SSR con nota protocollo n. 0505366 del 10/05/2023 e nota protocollo n. 0508997 del 11/05/2023 richiedendo esclusivamente il finanziamento per la migrazione a valere sull'investimento

1.1, ovvero verso infrastruttura PSN (Polo Strategico Nazionale);

che, per il perfezionamento della candidatura all'avviso di che trattasi, è stato richiesto il codice CUP G31C23000840006, inserito sulla piattaforma https://padigitale2026.gov.it nei tempi previsti dall'avviso stesso;

PRESO ATTO che in esito alla candidatura all'avviso pubblico multimisura pubblicato sulla piattaforma https://padigitale2026.gov.it, in data 22/08/2023, è stato notificato alla scrivente Azienda il decreto di finanziamento n. 48 - 4/2023 - PNRR del Dipartimento per la Trasformazione Digitale, che ha assegnato a questa ASL un finanziamento di € 1.358.595,00 per la migrazione dei propri servizi critici ed ordinari verso infrastruttura PSN (Polo Strategico Nazionale);

che il finanziamento di cui al Decreto n. 48 - 4/2023 - PNRR, così come stabilito ai commi 3 e 4 dall'art. 1 dell'Avviso pubblico multimisura PNRR – M1C1 – Investimenti 1.1 e 1.2 – ASL/AO, è definito come importo forfettario (*lump sum*) che "sarà erogato in un'unica soluzione a seguito del perfezionamento delle attività di migrazione al cloud", nelle modalità indicate all'art.13 ("Modalità di erogazione e rendicontazione");

DATO ATTO che in riscontro alla nota regionale prot. U.1159095.16-10-2023, recante ad oggetto "Avviso pubblico multimisura PNRR - M1C1 - Investimenti 1.1 e 1.2 - ASL/AO. Richiesta avvio rilevazione sui costi cessanti e attività di coordinamento degli interventi di migrazione delle ASL/AO", la scrivente Azienda ha trasmesso con nota prot. n. 44072 del 31-10-2023 le informazioni in merito ai costi cessanti derivanti dal completamento della migrazione al PSN e il questionario sui servizi di sicurezza;

che con nota prot. 1457255 del 14/12/2023 la Direzione regionale salute ed integrazione sanitaria della Regione Lazio ha formalmente richiesto al Dipartimento per la Trasformazione Digitale, con riferimento all'avviso multimisura in parola, una proroga dei tempi di caricamento dei contratti delle AA.SS. regionali;

che nella citata nota regionale era inoltre specificato che "le ASL/AO che non hanno ricevuto il Progetto dei Fabbisogni prevedono di determinare la negoziazione con il fornitore entro 10 giorni dalla ricezione del Progetto e di chiudere l'iter amministrativo interno/regionale per l'approvazione della spesa e per la firma del contratto entro la data del 15/02/2024";

che la ASL ROMA 5, in accordo con i referenti della società LazioCREA e con le altre ASL/AO regionali, in data 19/12/2023 ha presentato su piattaforma PA Digitale 2026 domanda di proroga dei tempi di caricamento del contratto con la società PSN Spa;

che in data 20/12/2023 la suddetta richiesta di proroga è stata approvata dal Dipartimento per la Trasformazione Digitale;

che con nota prot. n. 52440 del 21/12/2023 questa Azienda ha trasmesso al Polo Strategico Nazionale S.p.A il Piano dei Fabbisogni per la migrazione all'indirizzo PEC convenzione.psn@pec.polostrategiconazionale.it, così come previsto dalle procedure di cui al sito https://www.polostrategiconazionale.it/obiettivo-cloud/come-aderire/, al fine di ricevere il relativo Progetto dei Fabbisogni e tutti i documenti ad esso collegati per la contrattualizzazione;

che nel Piano dei Fabbisogni sopra citato sono stati inseriti, come da indicazioni regionali, soltanto i servizi relativi alla migrazione degli applicativi al PSN e il dimensionamento dell'infrastruttura in Cloud necessaria ad erogarli;

VISTI Il Progetto dei Fabbisogni codice n. PSN-SDE-CONV22-001-2023-0000004733471009-PPdF-PIR1 trasmesso dal Polo Strategico Nazionale S.p.A in data 06/02/2024 e acquisito a protocollo aziendale con n. 6133 del 06/02/2024, contenente la proposta tecnico-economica relativa all'esigenza espressa dall'ASL ROMA 5 mediante il suddetto Piano dei Fabbisogni, che unito al presente atto ne forma parte integrante e sostanziale come Allegato 1;

i seguenti allegati, trasmessi unitamente al citato Progetto dei Fabbisogni:

- Allegato 1 Schema di contratto;
- Allegato 6.1 Schema di Nomina Responsabile al Trattamento dei dati;
- Allegato 6.2 Misure tecniche di sicurezza;
- Allegato 7 Richiesta fideiussione;

DATO ATTO che il suddetto Progetto del Piano dei Fabbisogni prevede:

- il completamento della migrazione dei servizi critici ed ordinari erogati dalla scrivente Amministrazione entro otto mesi dalla sottoscrizione, in linea con le tempistiche previste dall'Avviso pubblico relativo al finanziamento PNRR;
- un costo una tantum per i servizi di migrazione di € 955.179,76 Iva esclusa, pari ad € 1.165.319,31 Iva inclusa, comprensivo di tutti i servizi di Analisi & discovery, setup, migrazione e collaudo;
- un canone annuale per i servizi infrastrutturali di € 324.243,96 Iva esclusa, pari ad € 395.577,63 Iva inclusa;

che, come da indicazioni della Direzione Regionale Salute e Integrazione Sociosanitaria della Regione Lazio, il Progetto del Piano dei Fabbisogni così come sopra indicato è stato condiviso nei contenuti tecnici, con esito positivo, tra il Direttore della UOC ICT della ASL Roma 5 e LAZIOcrea S.p.A.;

che con nota prot. 6306 del 07/02/2024, l'Azienda ha trasmesso alla Direzione Regionale Salute e Integrazione Sociosanitaria e alla Direzione Regionale per l'Innovazione Tecnologica e Trasformazione Digitale della Regione Lazio richiesta di autorizzazione alla stipula del contratto di utenza con la società PSN Spa in virtù del Progetto del Piano dei Fabbisogni ricevuto in data 06/02/2024, specificando che, salvo diverse indicazioni da parte dell'Amministrazione Regionale, al fine di rispettare le scadenze del finanziamento PNRR e l'obiettivo di migrazione in cloud, la ASL Roma 5 avrebbe proceduto alla contrattualizzazione e al caricamento della relativa documentazione sul portale Padigitale 2026 entro e non oltre il giorno 15/02/2024;

CONSIDERATO che, in relazione alla nota prot. n. 6306 di cui sopra, l'amministrazione regionale non ha trasmesso diverse indicazioni e altre osservazioni;

DATO ATTO che i costi derivanti dalla sottoscrizione della concessione per l'adesione al polo Strategico Nazionale, nei dieci anni di vigenza contrattuale, saranno di € 4.197.619,36 (oltre IVA), complessivamente pari ad € 5.121.095,62, IVA inclusa;

che, rispetto al costo complessivo sopra indicato, per il primo anno di contratto si prevede un costo di € 1.279.423,72 Iva esclusa, pari ad € 1.560.896,94 Iva inclusa;

che la quota relativa al canone infrastrutturale, pari a € 395.577,63 (IVA compresa), diverrà costo ricorrente per tutto il periodo di durata del contratto di che trattasi (10 anni, con clausola rescissoria a 3 anni);

che, per quanto sopra riportato, il Quadro Economico complessivo di affidamento è il seguente:

Descrizione servizio	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Servizi di migrazione (U.T.)	€ 955.179,76	€ -	€ -	€ -	€ -	€ -	€ -	€ -	€ -	€ -
Servizi infrastrutturali	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96	€ 324.243,96
Totale IVA Compresa	€ 1.560.896,94	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63	€ 395.577,63

che l'intervento è parzialmente finanziato nell'ambito del PNRR - Missione 1 - Componente 1 - Investimento 1.1 "Infrastrutture Digitali" ASL/AO (MARZO 2023);
che il finanziamento di cui al Decreto n. 48-4/2023-PNRR, pari ad € 1.358.595,00, sarà erogato in un'unica soluzione, solo nel caso in cui le attività di migrazione al cloud saranno perfezionate entro il giorno 22/10/2024;

che in caso di completamento della migrazione nei tempi previsti dal Progetto del Piano dei Fabbisogni codice n. PSN-SDE-CONV22-001-2023-0000004733471009-PPdF-PIR1, il costo dei servizi per il primo anno di contratto, pari ad € 1.560.896,94 IVA inclusa, **non** sarà interamente coperto dal suddetto finanziamento;

RITENUTO opportuno procedere all'adesione al Polo Strategico nazionale autorizzando la firma della relativa concessione, per una durata di dieci anni, a favore di Polo Strategico nazionale S.p.A., già concessionaria della Convenzione di concessione stipulata, ai sensi degli artt. 164, 165, 179, 180, comma 3, 183, comma 15, del d.lgs. n. 50 del 2016, in data 24 agosto 2022 tra Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – e la società di progetto Polo Strategico Nazionale Spa, con sede legale in Roma, via G. Puccini n.6, Codice Fiscale e Partita IVA 16825251008, per la prestazione da parte del Concessionario in favore delle singole Amministrazioni Utenti, in maniera continuativa e sistematica, di un Catalogo dei 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";

DATO ATTO che, per la presente procedura è stato acquisito dal sito dell'Autorità di Vigilanza sui Contratti Pubblici il CIG A04E9917A2 derivato dal CIG 9066973ECE;

PROPONE

Per le motivazioni espresse in premessa che si intendono qui riportate:

1. di approvare il Progetto dei Fabbisogni codice identificativo n. PSN-SDE-CONV22-001-2023-0000004733471009-PPdF-PIR1, così come trasmesso dalla società PSN Spa, unitamente agli allegati: Allegato 1 Schema di contratto, Allegato 6.1 Schema di Nomina Responsabile al Trattamento dei dati, Allegato 6.2 Misure tecniche di sicurezza, Allegato 7 Richiesta fideiussione, acquisito a protocollo aziendale con n. 6133 del 06/02/2024 allegato al presente provvedimento a farne parte integrante e sostanziale come Allegato 1;
2. di procedere alla stipula del contratto di utenza con la società PSN Spa, per la durata di anni 10 (dieci), con clausola di rescissione al terzo anno e per un importo pari ad € 4.197.619,36 Iva esclusa, pari ad € 5.121.095,62 Iva inclusa;
3. di dare atto che la presente procedura è identificata all'ANAC con CIG Derivato A04E9917A2;

4. di disporre che le quote di costo eccedenti il finanziamento di cui al CUP G31C23000840006 siano poste a carico del bilancio dell'Azienda;

5. di trasmettere il presente atto alla UOC Bilancio e Contabilità per l'imputazione dei relativi costi sul conto 502020106 "servizi di assistenza informatica", sui rispettivi anni di competenza, secondo lo schema seguente:

   - sull'anno 2024, per un costo totale, IVA compresa, pari a € 1.560.896,94, così ripartito:
     - quanto ad € 202.301,94 a carico del bilancio aziendale;
     - quanto ad € 1.358.595,00 a valere sui finanziamenti di cui agli interventi Piano Nazionale Ripresa e Resilienza (PNRR) – Missione 1 - Componente 1 – Investimento 1.1 "Infrastrutture Digitali";
   - sull'anno 2025, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2026, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2027, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2028, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2029, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2030, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2031, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2032, per un costo totale, IVA compresa, pari a € 395.577,63;
   - sull'anno 2033, per un costo totale, IVA compresa, pari a € 395.577,63;

6. di indicare quale Responsabile unico del procedimento il Dott. Luca Centurelli e Direttore esecutivo del contratto (DEC) la Dott.ssa Maria Fatima Pellegrino;
7. di rinviare a successivo provvedimento, in esito all'adeguamento al D.Lgs 36/2023 del Regolamento aziendale sugli incentivi per le funzioni tecniche, la definizione delle quote da accantonare a tale scopo;
8. di dare mandato alla UOC IT di provvedere, per quanto di competenza, alla gestione del rapporto contrattuale e alla liquidazione delle competenze effettivamente spettanti per il periodo di vigenza contrattuale;
9. di disporre che il presente atto venga pubblicato nell'Albo Pretorio on-line aziendale ai sensi dell'Art. 32 comma 1 della Legge n. 69 del 18 giugno 2009;

Attesta, altresì, che la presente proposta, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è legittima e pienamente conforme alla normativa che disciplina la fattispecie trattata.

Il Direttore f.f. UOC I.T.
Dott. Luca Centurelli

SULLA SUPERIORE PROPOSTA VENGONO ESPRESSI

Parere Favorevole
Data 08 FEB. 2024

Il Direttore Amministrativo
Dott. Filippo Coiro

Parere FAVOREVOLE
Data 08 FEB. 2024

Il Direttore Sanitario f.f.
Dott. Franco Cortellessa

IL DIRETTORE GENERALE

Dott. Giorgio Giulio Santonocito, nominato con Decreto del Presidente della Regione Lazio n. T00096 del 11 luglio 2022

Vista la superiore proposta di deliberazione, formulata dal Dott. Luca Centurelli, Direttore f.f. UOC IT, che, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, ne ha attestato la legittimità e la piena conformità alla normativa che disciplina la fattispecie trattata;

Ritenuto di condividere il contenuto della medesima proposta;

DELIBERA

Di approvare la superiore proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata e sottoscritta dal Dott. Luca Centurelli, Direttore f.f. UOC IT;

di disporre che il presente atto **venga pubblicato** nell'Albo Pretorio on-line aziendale ai sensi dell'Art. 32 comma 1 della Legge n. 69 del 18 giugno 2009;

Il Direttore Amministrativo
Dott. Filippo Coiro

Il Direttore Sanitario f.f.
Dott. Franco Cortellessa

Il Direttore Generale
Dott. Giorgio Giulio Santonocito

PUBBLICAZIONE

Copia della presente deliberazione è stata affissa all'Albo delle Pubblicazioni presso la Sede dell'Azienda Sanitaria Locale Roma 5 in data : 06 FEB. 2024

Il Direttore f.f. U.O.C. Affari Generali e Legali
(Avv.to Enzo Fasani)

L'addetto alla Pubblicazione

Per copia conforme all'originale, per uso amministrativo

Il Direttore f.f. U.O.C. Affari Generali e Legali
(Avv.to Enzo Fasani)

Tivoli, _____

ALLEGATO 1

Polo Strategico Nazionale

Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 06/02/2024 14:14
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

Concessione per la realizzazione e la 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

PROGETTO DEL PIANO DEI FABBISOGNI

SISTEMA SANITARIO REGIONALE

ASL ROMA 5

PSN-SDE-CONV22-001-2023-0000004733471009-PPdF-P1R1

Polo Strategico Nazionale

SOMMARIO

Indice delle tabelle

STATO DEL DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

TITOLO DEL DOCUMENTO		
Descrizione Modifica	Revisione	Data
Prima Emissione	1	30/01/2024

Tabella 1: Informazioni Documento

Autore	
Team di lavoro PSN	Unità operative Solution Development, Technology Hub e Sicurezza

Tabella 2: Autore

Revisore	
PSN Solution team	n.a.

Tabella 3: Revisore

Approvazione	
PSN Solution team PSN Commercial team	Paolo Trevisan Riccardo Rossi

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Solution Development
- Funzione Technology Hub
- Funzione Sicurezza
- Referente Servizio
- Direttore Servizio

ESTERNA A:

- Referente Contratto Esecutivo ASL Roma 5 Luca Centurelli
  - Email: luca.centurelli@aslroma5.it
- Referente Tecnico ASL Roma 5 Luca Centurelli
  - Email: luca.centurelli@aslroma5.it

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del PSN relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della 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. Quanto descritto, è stato redatto in conformità alle richieste del *ASL Roma 5* di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (2023-0000004733471009-PdF-P1R1).

2 AMBITO

L'ASL Roma 5 ha l'obiettivo di ottenere il passaggio in sicurezza dei propri sistemi sulla nuova piattaforma cloud resa disponibile dal PSN: l'importanza dei servizi erogati rende necessario minimizzare l'impatto sull'attuale architettura applicativa, mettendo in sicurezza i sistemi e attivando e/o aggiornando gli attuali strumenti di monitoraggio e controllo.

Allo scopo di garantire una migrazione efficace, traguardando quindi l'operatività dei servizi sulla nuova infrastruttura, il PSN delinea un iter progettuale, coerente con le richieste espresse tramite l'emissione del Piano dei Fabbisogni, che prevede:

- Predisposizione risorse cloud
- Servizi di migrazione in modalità Lift & Shift e Replatform se necessario, per le componenti applicative conformi ai requisiti minimi PSN e con preliminare aggiornamento dei sistemi operativi per le componenti applicative legacy

L'attività di migrazione sarà corredata da task specifici di

- PMO
- Infrastructure Assessment
- Network Assessment
- Application Assessment
- Definizione documentata del piano di migrazione di dettaglio e dei piani di Failover/Failback
- Predisposizione networking per connessione tra AO San Giovanni e PSN
- Setup infrastruttura Cloud
- Setup servizi PAAS, File Share, Storage Account, Object Storage
- Setup servizi network, DFW e di reverse proxy
- Configurazione servizi HA intra-region e BackUp
- Implementazione/Configurazione script e procedure di automazione di Failover/Failback intra-region
- Test e collaudo infrastrutturale e applicativo
- Ratifica e Certificazione Test di Failover/Failback infrastrutturale

Lo svolgimento delle attività sarà corredato, in linea con la pianificazione condivisa con l'Amministrazione, dal rilascio dei seguenti deliverable:

- Disegno infrastrutturale (server, storage, network, ...)
- Piano di migrazione
- Test e collaudi migrazioni applicative

I servizi descritti dovranno essere applicati a tutti gli applicativi oggetto di migrazione, anche in considerazione dei livelli di integrazione esistenti tra le differenti applicazioni aziendali, sia a livello locale che a livello regionale.

Nella tabella seguente vengono riportati i servizi oggetto di migrazione nel presente Progetto:

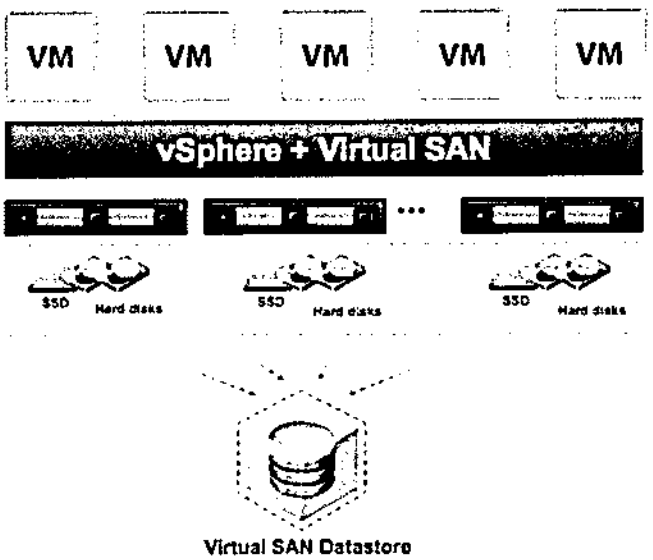
Applicativo ASL	Servizio Amministrazione	Livello di Classificazione	Tipologia di Migrazione
Modulab	ATTIVITÀ DIAGNOSTICA	CRITICO	Lift&Shift
SGSL	SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	ORDINARIO	Lift&Shift
SIS4CARE			
URP BACK OFFICE	RAPPORTI CON L'UTENZA - URP	ORDINARIO	Lift&Shift
URP FRONT END			
TDMS	ASSISTENZA A PARTICOLARI CATEGORIE	CRITICO	Re-Platform
TDMS-DB			
EUSIS	CONTABILITÀ, BILANCIO E CONTROLLO	ORDINARIO	Lift&Shift
DATABASE PROD			
EUSIS TEST			
DIGITGO	GESTIONE DOCUMENTALE	ORDINARIO	Lift&Shift
DIGITGO TEST			
DATABASE TEST			
COOPERA			Lift&Shift
JSISAN	RICOVERO ORDINARIO PER ACUTI	CRITICO	Lift&Shift
JSISAN TEST			
SIS4CARE			Lift&Shift
JSISAN-MIRTH	ASSISTENZA FARMACEUTICA	CRITICO	Lift&Shift
JSISAN-DB			
JSISAN DB TEST			
JOBTIME	PERSONALE	ORDINARIO	Lift&Shift
COOPERA	PROTOCOLLO	ORDINARIO	Lift&Shift
SIS4CARE	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	Lift&Shift
SIS4CARE	DAYSURGERY	CRITICO	Lift&Shift
SIS4CARE	DAY HOSPITAL	CRITICO	Lift&Shift
SIS4CARE	RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	CRITICO	Lift&Shift
SIS4CARE	FASCICOLO SANITARIO REGIONALE	CRITICO	Lift&Shift
ZEXTRAS CARBONIO	PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	ORDINARIO	Lift&Shift
SITP WEB	COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	ORDINARIO	Lift&Shift
OSLO	CONTABILITÀ, BILANCIO E CONTROLLO	ORDINARIO	Lift&Shift

La migrazione verso il PSN avverrà per tutti i servizi in "modalità A" - Trasferimento in sicurezza dell'infrastruttura IT"; tuttavia, in ragione dei vincoli tecnici dell'infrastruttura PSN, per alcune applicazioni potrebbe rendersi necessario effettuare attività di aggiornamento che prevedono attività di Upgrade SO a cura cliente, tali attività verranno effettuate prima della migrazione verso il PSN sui sistemi on-premise.

2.1 Contesto di riferimento

Ad oggi le infrastrutture e le piattaforme applicative eroganti servizio per la ASL Roma 5, si trovano locate presso il data center sito in Via Acquaregna 1/15 - 00019 Tivoli (RM).

A seguire uno schema architetturale relativo alla piattaforma ospitante i servizi erogati:



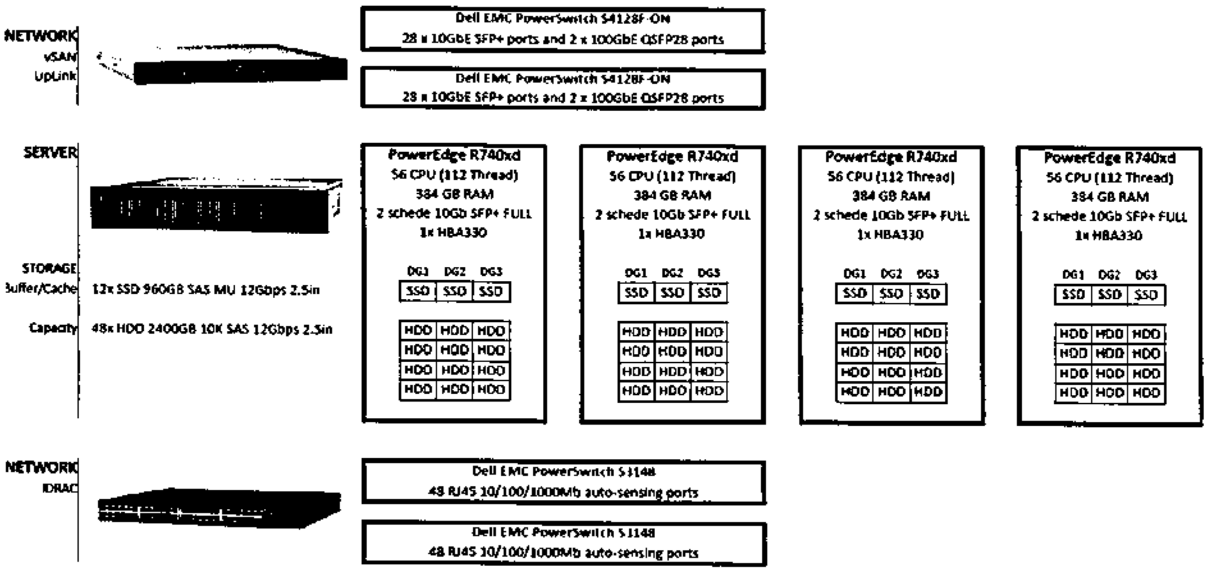


Figura 1 Infrastruttura As-Is

Come si evince dallo schema è presente un servizio di DR per solo 15 VM su 52.

Inoltre, è presente una componente computazionale quasi completamente dedicata alla piattaforma di virtualizzazione dei server eroganti i servizi per la ASL Roma 5, che è suddivisa su due architetture gestite ognuna da un vCenter dedicato.

Sono presenti due dispositivi storage così costituiti:

- NAS SYNOLOGY RS2418RP+ con DSM 7.1.1-42962 Update 6 (31.4 TB totali di cui 24.2 utilizzati)
- SAN PowerVault MD3620f con 48 dischi 1.2TB ciascuno [57.6 TB totali di cui 39 TB assegnati a VMware 5.5 (di cui 31.12 TB liberi)]

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Titolo	Documento consegnato	Versione	Data versione
#1	Piano dei Fabbisogni di Servizio	PSN_Piano dei Fabbisogni_v1.0	1.0	01.12.2022
#2	Piano di Sicurezza	PSN-SDE-CONV22-001-PianoSicurezza v.1.0 Allegati: PSN - Processo IM v.03 2.C Qualificazione Servizi Cloud 2.B Fornitore Servizio Cloud 2.A Soggetto Infrastruttura Digitale	1.0	22.12.2022
#3	Piano di Qualità	PSN-SDE-CONV22-001-Piano della Qualità	1.0	22.12.2022
#4	Piano di Continuità Operativa	PSN-SDE-CONV22-001-Piano di Continuità Operativa ver.1.0	1.0	22.12.2022

Tabella 5: Documenti Contrattuali

3.2 DOCUMENTI DI RIFERIMENTO

La seguente tabella riporta i documenti che costituiscono il riferimento a quanto esposto nel seguito del presente documento.

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022	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"
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato A)	Capitolato Tecnico e relativi annessi – Capitolato Servizi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato B)	"Offerta Tecnica" e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato C)	"Offerta economica del Fornitore – Catalogo dei Servizi" e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato D)	Schema di Contratto di Utenza
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato H)	Indicatori di Qualità
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato I)	Flussi informativi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato L)	Elenco dei Servizi Core, no Core e CSP

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

Riferimento	Codice	Titolo
Template Progetto del Piano dei Fabbisogni	PSN- TMPL- PGDF	Progetto del Piano dei Fabbisogni Template

Tabella 7: Documenti Applicabili

4 ACRONIMI

La seguente tabella riporta le descrizioni o i significati degli acronimi e delle abbreviazioni presenti nel documento.

Acronimo	Descrizione
CMP	Cloud Management Platform
CSP	Cloud Service Provider
DB	DataBase
DR	Disaster Recovery
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PSN	Polo Strategico Nazionale
VM	Virtual Machine
WORM	Write Once, Read Many

Tabella 8: Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

Uno degli obiettivi del PSN è la riduzione dei consumi energetici è pertanto necessario, nell'ottica dell'energy control, stabilire i consumi energetici dell'infrastruttura dell'Amministrazione. Questa verrà fatta assumendo come valore di riferimento il consumo (misurato o stimato sulla base dei valori di targa) annuo dell'infrastruttura prima che questa venga migrata. Seguirà una valutazione circa l'utilizzo delle risorse HW e SW impegnate nel PSN con il preciso scopo di contenerne i consumi.

5.1 SERVIZI PROPOSTI

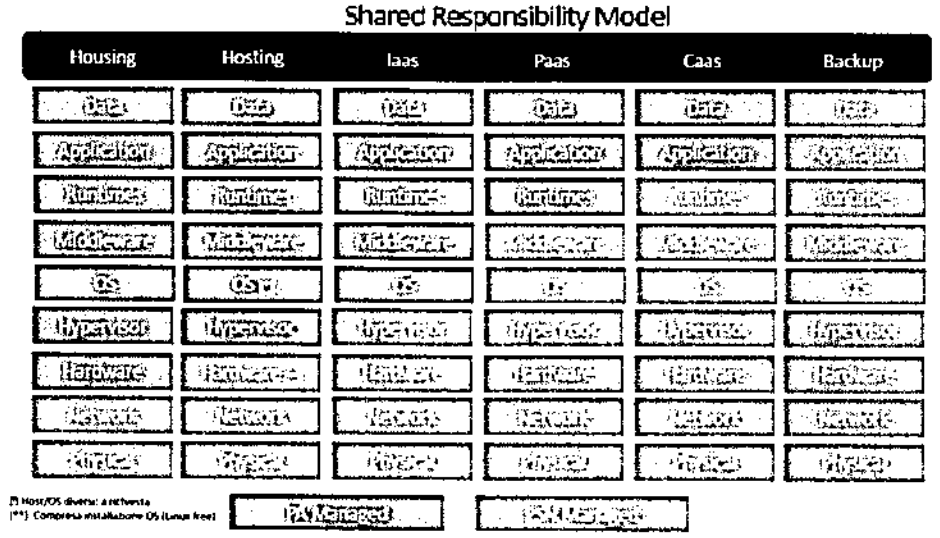
Di seguito si riporta una sintesi delle soluzioni individuate per soddisfare le esigenze dell'Amministrazione.

Servizio	Importo
Industry Standard	Housing
Industry Standard	Connettività
Industry Standard	IaaSharedHA
Industry Standard	IaaSStorageHA
Industry Standard	Data Protection: Backup
Industry Standard	Data Protection: Golden copy protetta
Servizi di Migrazione	
Servizi Professionali	IT Infrastructure Service Operation

Tabella 9: Servizi Proposti

L' amministrazione, in questa fase non richiede il servizio di Disaster Recovery.

Di seguito, è mostrata la matrice di responsabilità nell'ambito della gestione dei servizi migrati su PSN:



Si riporta di seguito la classificazione dei dati per i servizi/applicazioni che fornisce un quadro sintetico del progetto di migrazione dell'Amministrazione.

Servizio dell'amministrazione	Classificazione
PRONTO SOCCORSO	CRITICO
ASSISTENZA FARMACEUTICA	CRITICO
RICOVERO ORDINARIO PER ACUTI	CRITICO
ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO
DAYSURGERY	CRITICO
DAY HOSPITAL	CRITICO
RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	CRITICO
ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO
SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	ORDINARIO
FASCICOLO SANITARIO REGIONALE	CRITICO
ATTIVITÀ DIAGNOSTICA	CRITICO
ASSISTENZA A PARTICOLARI CATEGORIE	CRITICO
RAPPORTI CON L'UTENZA - URP	ORDINARIO
COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	ORDINARIO
PROTOCOLLO	ORDINARIO
GESTIONE DOCUMENTALE	ORDINARIO
PERSONALE	ORDINARIO
CONTABILITÀ, BILANCIO E CONTROLLO	ORDINARIO
ACQUISTI	ORDINARIO
PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	ORDINARIO

Tabella 10: Classificazione Servizi

5.2 INDUSTRY STANDARD

5.2.1 Housing

5.2.1.1 Descrizione del servizio

Il Servizio Industry Standard Housing è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di aree esclusive all'interno dei Data Center del PSN, 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, atte ad ospitare le infrastrutture IT e TLC di proprietà dell'Amministrazione, nonché di eventuali variazioni in corso d'opera.

5.2.1.2 Personalizzazione del servizio

In ambito Housing si prevede la messa disposizione dei seguenti servizi:

Codice	Tipologia	Elemento	Qtà	Note
HOUSING05	Housing	IP Pubblici /29 (8 indirizzi)	2	
HOUSING03	Housing	Rilancio connettività (fibra monomodale)	2	

Tabella 11: Housing

5.2.1.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.1.4 Specifiche di collaudo

Per le modalità di svolgimento delle prove di Collaudo e di Test, previste per il servizio in oggetto, finalizzate a verificare la conformità del Servizio standard offerto a catalogo, si rimanda, alla documentazione ufficiale di collaudo dei Servizi PSN effettuato dal Dipartimento della Trasformazione Digitale, disponibile in un'apposita sezione del Portale della Fornitura.

5.2.2 Connettività

5.2.2.1 Descrizione del servizio

Il Servizio Industry Standard Connettività che permette una connettività diretta verso il PSN al fine di avere un percorso preferenziale.

5.2.2.2 Personalizzazione del servizio

In ambito Connettività si prevede la messa disposizione dei seguenti servizi:

Codice	Tipologia	Elemento	Qtà	Note
CONN01	Connettività	Tecnologia Gbe MPLS, profilo Silver 1000, TIR L2/L e outsourcing	2	

Tabella 12: Connettività

La realizzazione dei collegamenti verrà avviata previa verifica del cliente della effettiva indisponibilità della rete RANSAN della regione Lazio attualmente in corso di ampliamento e che prevede il collegamento al Cloud PSN.

5.2.2.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore". Inoltre, i collegamenti verranno attivati solo se la Rete Ransan (fornita da Regione Lazio) non fosse disponibile in tempo utile alla migrazione.

5.2.2.4 Specifiche di collaudo

Per le modalità di svolgimento delle prove di Collaudo e di Test, previste per il servizio in oggetto, finalizzate a verificare la conformità del Servizio standard offerto a catalogo, si rimanda, alla documentazione ufficiale di collaudo dei Servizi PSN effettuato dal Dipartimento della Trasformazione Digitale, disponibile in un'apposita sezione del Portale della Fornitura.

5.2.3 *Infrastructure as a Service*

5.2.3.1 *Descrizione del servizio*

I servizi di tipo Infrastructure as a Service (IaaS) sono servizi *Core* e 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.

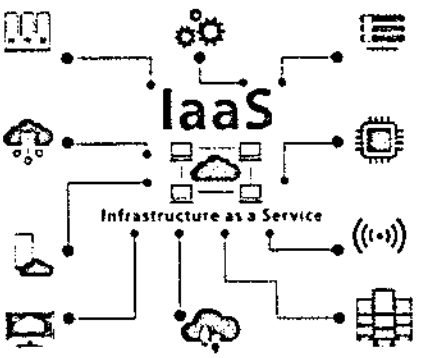


Figura 2 Infrastructure as a Service

Il servizio IaaS è suddiviso in:

- IaaS Private: consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e dedicata, in grado di ospitare tutte le applicazioni in carico all'Amministrazione 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.

  Il PSN è responsabile della gestione dell'infrastruttura sottostante e rende disponibile gli strumenti e le console per la gestione in autonomia degli ambienti fisici e virtuali contrattualizzati.

- IaaS Shared: consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e condivisa, in grado di ospitare tutte le applicazioni in carico all'Amministrazione 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.

  In questo caso, l'Amministrazione acquisisce il pool di risorse (vCPU, vGB di RAM, vGB di Storage) virtuali e il PSN è responsabile della gestione dell'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

5.2.3.2 Personalizzazione del servizio

La proposta architetturale prevista sull'infrastruttura PSN sfrutta le caratteristiche specifiche delle soluzioni Industry, sfruttando la continuità con la piattaforma VMWare per garantire l'erogazione dei workload oggetto di migrazione.

La progettualità specifica prevede la composizione di un disegno architetturale che possa indirizzare le esigenze di dialogo tra le diverse componenti di ogni servizio e la fruibilità degli stessi da parte dell'Amministrazione.

Codice	Tipologia	Elemento	Qtà	Note
IAAS16	IaaSSharedHA	Pool Large	8	Risorse per migrazione VM
IAAS07	IaaSStorageHA	Storage HP Encrypted	40	Storage per VM con dati critici/DB
IAAS03	IaaSStorageHA	Storage High Performance	41	Storage per VM con dati ordinari
IAAS04	IaaSStorageHA	Storage Standard Performance	75	Storage per VM con dati ordinari

Tabella 13: IaaS Shared e IaaS Storage

La nuova infrastruttura Cloud è stata progettata sulla base delle risorse necessarie per garantire prestazioni ed efficienza dei domini applicativi. In fase di finalizzazione del piano di migrazione le risorse computazionali previste saranno distribuite al fine di garantire l'erogazione dei servizi e segregate tra i vari ambienti e domini applicativi.

5.2.3.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.3.4 Specifiche di collaudo

Per le modalità di svolgimento delle prove di Collaudo e di Test, previste per il servizio in oggetto, finalizzate a verificare la conformità del Servizio standard offerto a catalogo, si rimanda, alla documentazione ufficiale di collaudo dei Servizi PSN effettuato dal Dipartimento della Trasformazione Digitale, disponibile in un'apposita sezione del Portale della Fornitura.

5.2.4 Data Protection e Disaster Recovery

L'amministrazione ha scelto di attivare il servizio di Data Protection Backup e di non attivare il DR per i servizi critici, come previsto da ACN, poiché ne ritiene prematura l'attivazione. L'amministrazione si riserva la predisposizione di un nuovo PdF a valle della messa in produzione delle proprie applicazioni.

5.2.4.1 Data Protection: Backup

Il servizio permette di proteggere le applicazioni critiche facendo leva su un servizio di backup che è allo stato attuale il modo migliore per garantire la continuità operativa. È fondamentale impostare per tutte le attività, 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 di ripristinare immediatamente l'operatività di tutti i sistemi, riducendo al minimo – o addirittura azzerando – il downtime.

Trattandosi di un Servizio «self-managed», l'utente ha completa autonomia di gestione nella definizione della policy di backup. Il servizio di backup standard prevede di effettuare il backup dello storage base (100GB) previsto per ogni istanza. Per tutti i backup sarà effettuata una ulteriore copia secondaria al completamento della copia primaria presso il Data Center secondario
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);
- 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-ofplace" 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

Il servizio di Backup è fatturato a canone annuale basato sulla quantità di spazio (TB) riservato al Cliente in fase di acquisto del servizio indipendentemente da quanto spazio sia stato occupato.

5.2.4.2 Personalizzazione del servizio

Il progetto prevede il servizio di backup per la copia dei dati che verranno migrati nel Cloud PSN relativamente agli ambienti IaaS descritti ai precedenti paragrafi.

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITÀ	NOTE
DP02	IndustryStandard	DataProtection	Backup	423	Risorse per Backup con configuratore BaaS con Policy Gold

Tabella 14-Backup

La quantità di dati grezzi oggetto di backup è di 47TB. Inoltre, si prevede di applicare le seguenti politiche di backup:

- Periodicità del full backup (giorni che intercorrono tra 2 full backup successivi) pari a 6 giorni.
- Periodicità del backup incrementale (giorni che intercorrono tra 2 backup incrementali successivi) pari a 1 giorno.
- Retention del backup (tempo in giorni prima di cancellare il backup più "vecchio") pari a 30 giorni.
- Percentuale dei dati sul full backup che si stima per ciascun backup incrementale pari al 10%.

In virtù delle suddette ipotesi il totale dello spazio disco riservare su PSN per il backup dei dati dell'Amministrazione è pari a 423TB.

In sintesi, si avranno a regime 6 full backup nel periodo di retention (escluso il primo) mentre il numero dei backup incrementali sarà pari a 30.

Lo spazio massimo di backup sarà di 423 TB, spazio strettamente necessario a garantire tale tipologia di storage primario. In caso di ulteriori fabbisogni sarà cura dell'amministrazione procedere con nuovo ordine.

5.2.4.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Nella tabella seguente viene mostrato il dimensionamento del servizio Industry Standard – Data Protection Backup.

[illegible]	[illegible]	[illegible]	[illegible]
DP02	DataProtection	Backup	423

Tabella 15. Servizio BaaS

Le specifiche per il backup sono coerenti con gli standard proposti dal PSN, prevedendo quindi un backup full settimanale e un backup incrementale quotidiano.

5.2.4.4 Data Protection: Golden copy protetta

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, il PSN mette a disposizione un servizio opzionale aggiuntivo che analizza i backup 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 e 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.

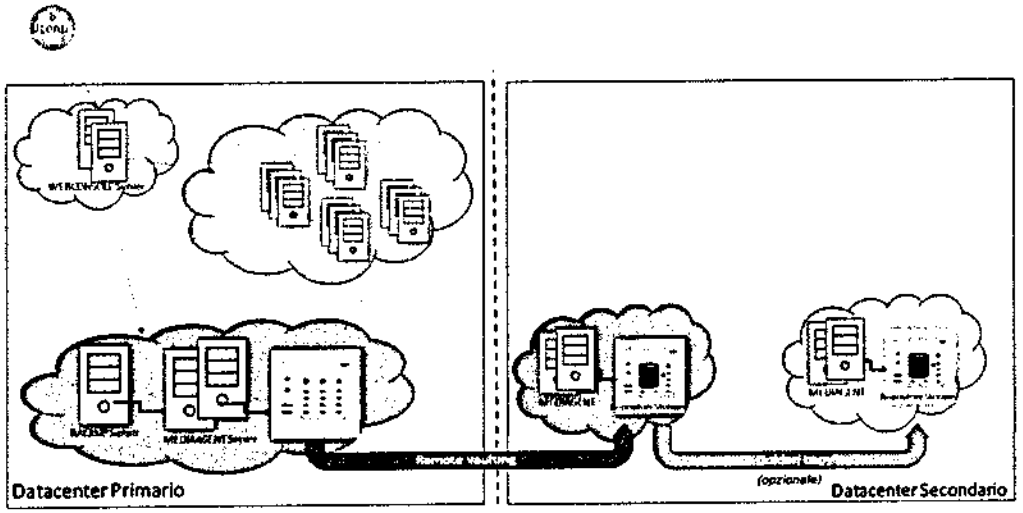


Figura 3 Architettura Funzionale Golden Copy

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.
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 del PSN;
- protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- replica in Region diverse e su canale cifrato.

5.2.4.5 *Personalizzazione del servizio*

Nella tabella seguente viene mostrato il dimensionamento del servizio Industry Standard – Data Protection Golden Copy.

Codice	Tipologia	Elemento	Qtà
DP03	DataProtection	Golden Copy	127

Tabella 16: Servizio BaaS - GC

5.2.4.6 *Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)*

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.4.7 *Specifiche di collaudo*

Per le modalità di svolgimento delle prove di Collaudo e di Test, previste per il servizio in oggetto, finalizzate a verificare la conformità del Servizio standard offerto a catalogo, si rimanda, alla

documentazione ufficiale di collaudo dei Servizi PSN effettuato dal Dipartimento della Trasformazione Digitale, disponibile in un'apposita sezione del Portale della Fornitura.

5.3 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.
Il 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 il PSN si avvarrà del supporto di secondo livello di specialisti di prodotto/tecnologia.

5.3.1 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".

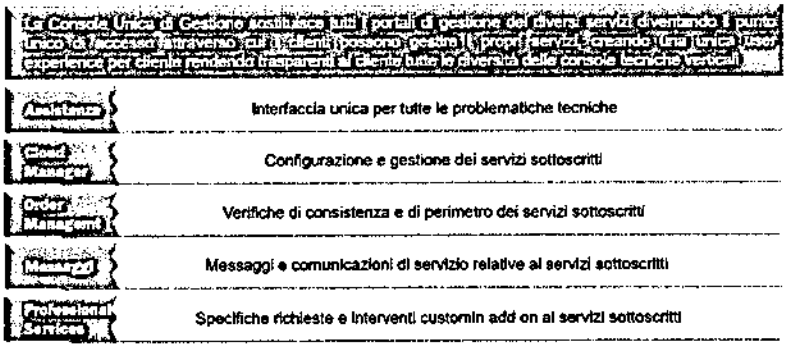


Figura 4 Funzionalità CU

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.

5.3.2 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".

5.3.3 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.).

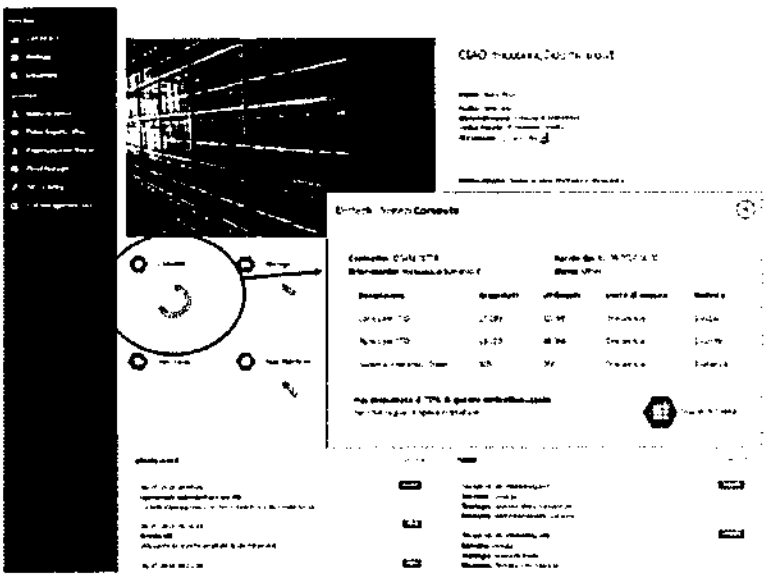


Figura 5 Dashboard CU

- 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.

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.

5.4 SERVIZI E PIANO DI MIGRAZIONE

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assessment effettuati 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 di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

- Un Project Manager Contratto di Adesione, che coordina le attività e collabora col referente che ogni singola PA dovrà indicare e mettere a disposizione;

- Un Technical Team Leader che segue tutte le fasi più strettamente legate agli aspetti operativi.

Si chiede alla PA la disponibilità di fornire uno o più referenti coi quali il Project Manager Contratto di Adesione e il Technical Team Leader del 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 PSN e PA.

Il Piano di Migrazione, che rappresenta un allegato parte integrante del presente documento, , è redatto adottando la metodologia basata sul framework EMG2C (Explore, Make, Go to Cloud), articolato in tre distinte fasi:

- Explore, che 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.
- Make, 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.
- Go, 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.

Gli step operativi in cui si articolano le suddette fasi sono:

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

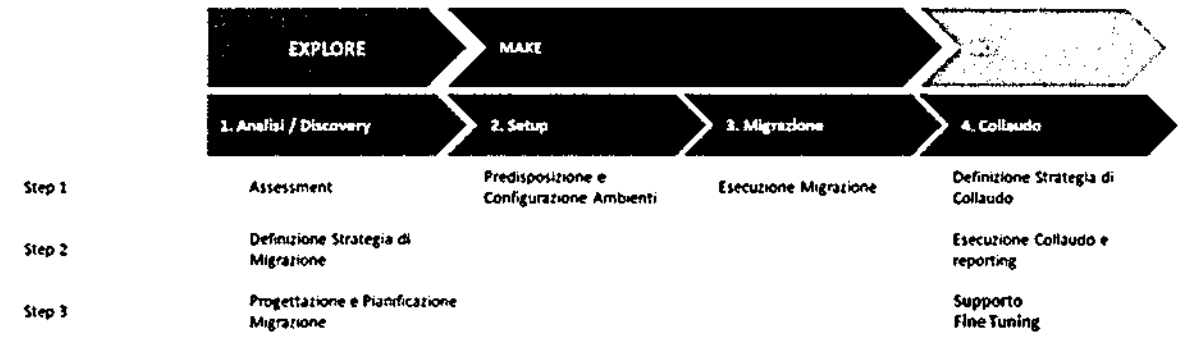


Figura 6: Servizio di Migrazione - Metodologia EMG2C

1. Analisi e Discovery

Il primo step consiste nell'Assessment, finalizzato alla raccolta di tutte le informazioni necessarie e utili alla corretta esecuzione della migrazione. Tali informazioni saranno raccolte tramite:

- Survey, tramite compilazione da parte degli stakeholder della Amministrazione di template e checklist condivisi.
- Interviste one-to-one con i referenti dell'Amministrazione per la raccolta di dati inerenti alle applicazioni da migrare e alle loro potenziali rischi/criticità.
- Document repository ossia raccolta di tutta la documentazione disponibile presso la Pubblica Amministrazione.
- Tools di Analisi e Discovery a supporto

In particolare, questa fase di occuperà di reperire le informazioni:

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 delle applicazioni e dell'ambiente da migrare;
i) Energy Optimization.

Inoltre, la Discovery ha lo scopo di raccogliere tutte le informazioni relative all' 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 migrate.
In funzione dei risultati dell'Assessment, si valuterà la strategia ottimale di migrazione verso l'ambiente target, in funzione dei seguenti driver:

- Ottimizzazione degli effort e dei tempi di migrazione.
- Minimizzazione dei rischi.

La fase di Analisi utilizzata per valutare le diverse strategie di Migrazione terrà conto anche del livello di maturità di adozione del Cloud della PA, delle dimensioni, complessità e conoscenza dei servizi della PA stessa.

Definita la strategia, si provvederà a dettagliare le attività necessarie a definire un master plan di tutti gli interventi necessari per implementare la migrazione prevista per la specifica Amministrazione; ciascun intervento sarà quindi declinato in un piano operativo.

2. Set-up

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 e si articola nelle seguenti fasi:

- Progettazione operativa e di dettaglio.
- Predisposizione dell'infrastruttura target presso i DC del PSN.
- Predisposizione dell'infrastruttura di networking relativa alla connessione tra la PA e i DC del PSN, se richiesta nel Piano dei Fabbisogni

Il completamento della fase di setup coincide con l'avvio della "gestione dei servizi"

3. Migrazione

Tale fase si articola nei seguenti step:

- 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 delle Policy di Sicurezza;
- Impostazione del monitoraggio.

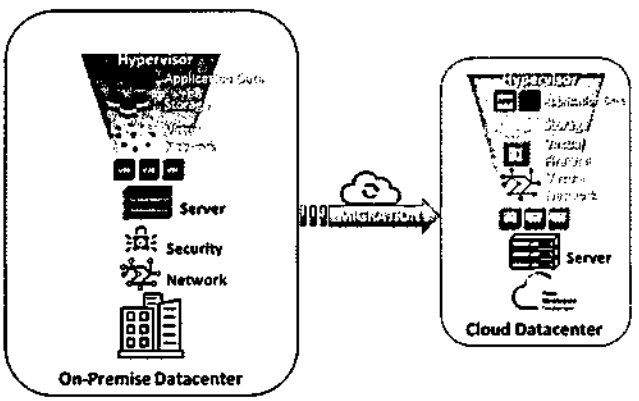


Figura 7 Migrazione

4. Collaudo

Definizione Strategia di Collaudo: tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo delle applicazioni migrate nell'ambiente target.

Esecuzione Collaudo: tale fase consiste nell'esecuzione dei test dei servizi PSN attivati e definiti in precedenza con la PA per certificare il Go Live delle applicazioni su ambiente target da un punto di vista infrastrutturale.

A valle del collaudo, sarà previsto un grace period temporaneo, da concordare con la Pubblica Amministrazione, durante il quale viene fornito un supporto alle operation del cliente per il fine tuning delle applicazioni migrate nell'ambiente target, in termini di prestazioni.

Nella seguente tabella sono indentificate il numero di server da migrare in base alla tipologia di applicativo:

Servizio dell'Amministrazione	Classificazione	VM
PRONTO SOCCORSO	CRITICO	0

ASSISTENZA FARMACEUTICA	CRITICO	3
RICOVERO ORDINARIO PER ACUTI	CRITICO	3
ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	1
DAYSURGERY	CRITICO	1
DAY HOSPITAL	CRITICO	1
RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	CRITICO	1
ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	1
SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	ORDINARIO	2
FASCICOLO SANITARIO REGIONALE	CRITICO	3
ATTIVITÀ DIAGNOSTICA	CRITICO	7
ASSISTENZA A PARTICOLARI CATEGORIE	CRITICO	2
RAPPORTI CON L'UTENZA - URP	ORDINARIO	2
COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	ORDINARIO	1
PROTOCOLLO	ORDINARIO	3
GESTIONE DOCUMENTALE	ORDINARIO	6
PERSONALE	ORDINARIO	4
CONTABILITÀ, BILANCIO E CONTROLLO	ORDINARIO	6
ACQUISTI	ORDINARIO	0
PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	ORDINARIO	6

Tabella 17: Wave Applicative

5.4.1 Piano di attivazione e Gantt

In questa sezione si riporta un diagramma di Gantt di massima per le attività previste nel progetto.

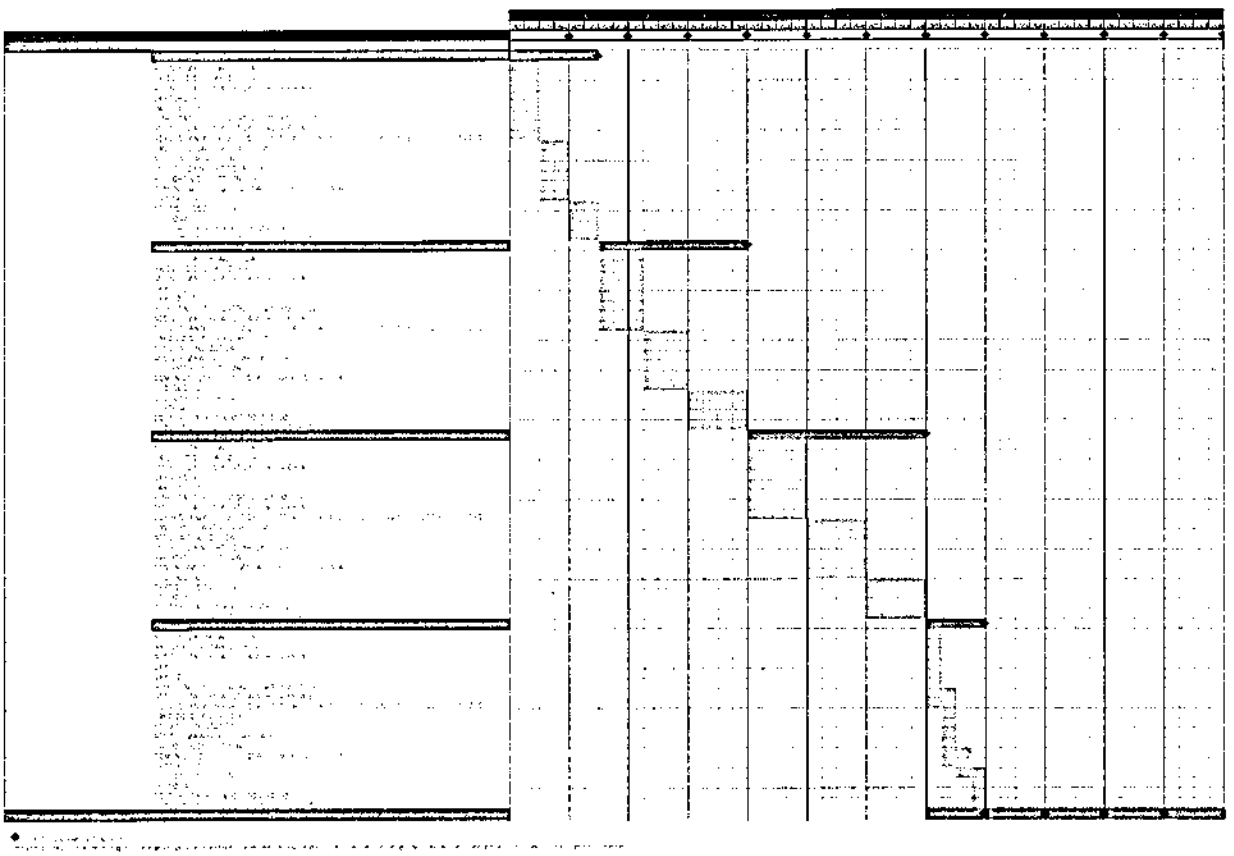


Figura 8 Gantt

5.5 SERVIZI PROFESSIONALI

Sono resi disponibili all'Amministrazione 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 proposti sono 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, viene proposto un team mix composto dai profili professionali elencati in precedenza.

5.5.1 *IT infrastructure service operations*

In seguito all'avvenuta migrazione, il PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni, ovvero dell'infrastruttura VM della PA. Pertanto, l'Amministrazione potrà decidere di affidare al PSN la gestione dell'ambiente tenendo per sé solamente la componente relativa al codice applicativo. Per il corretto svolgimento delle attività verrà reso disponibile, 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 il 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.

- 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 elencati in precedenza, in base all'ambiente dell'Amministrazione ed ai requisiti della stessa.

5.5.1.1 *Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)*

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

6 FIGURE PROFESSIONALI

PSN rende disponibili risorse professionali in grado di poter supportare l'Amministrazione nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-architect, re-platform), proseguendo nella fase di riavvio degli applicativi, regression test e terminando nel supporto all'esercizio.
Per ogni progetto viene individuato il mix di figure professionali necessarie, tra quelle messe a disposizione del PSN, che effettuerà le attività richieste. Si rimanda al par. 8 Configuratore per il dettaglio dell'effettivo impegno delle risorse professionali previste per tale progetto. Il team reso disponibile per questo progetto è composto dalle seguenti figure professionali, i cui profili sono di seguito descritti:

- 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 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
- 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.
- 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 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
- 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

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

7 SICUREZZA

All'interno del PSN è presente una Organizzazione di Sicurezza, con elementi caratteristici di autonomia e indipendenza. Tale unità è anche preposta alle attività aziendali rilevanti per la sicurezza nazionale ed è coinvolta nelle attività di governance, in particolare riguardo ai processi decisionali afferenti ad attività strategiche e di interesse nazionale.

Le misure tecniche ed organizzative del PSN sono identificate ed implementate ai sensi delle normative vigenti elaborate a cura dell'Organizzazione di Sicurezza, in particolare con riferimento alla sicurezza e alla conformità dei sistemi informatici e delle infrastrutture delle reti, in totale allineamento e coerenza con i criteri di accreditamento AgID relativi ai PSN.

L'Amministrazione non richiede l'esecuzione delle attività finalizzate ad "identificare il livello di maturità di sicurezza informatica AS-IS" - secondo le tre dimensioni di Governance, Detection e Prevention - così come previsto nell'esecuzione della "fase di assessment della Amministrazione target e definizione della strategia di migrazione" (Cfr. Convenzione - Relazione Tecnica Illustrativa, Par. 22.6.1 - Explore - fase di Analisi/Discovery - Step 1.1 Assessment - Data Collection & Analysis). In assenza di valutazione del livello di maturità di sicurezza, il PSN non potrà "identificare potenziali lacune e impatti su Organizzazione, Processi e Tecnologia al fine di definire le opportune remediation activities".

Con la sottoscrizione del presente Progetto del Piano dei Fabbisogni, l'Amministrazione accetta tutte le policy di sicurezza di PSN.
Le policy di sicurezza delle informazioni di PSN delimitano e regolano le aree di sicurezza applicabili ai Servizi PSN e all'uso che l'Amministrazione fa di tali Servizi. Il personale di PSN (compresi dipendenti, appaltatori e collaboratori a tempo determinato) è tenuto al rispetto delle prassi di sicurezza dei dati di PSN e di eventuali policy supplementari che regolano tale utilizzo o i servizi che forniscono a PSN.
Per i Servizi che non sono inclusi nella fornitura e per i quali l'Amministrazione autonomamente configura un comportamento di sicurezza, se non diversamente specificato, resta a carico dell'Amministrazione la responsabilità della configurazione, gestione, manutenzione e protezione dei sistemi operativi e di altri software associati a tali Servizi non forniti da PSN.

L'Amministrazione resta responsabile dell'adozione di misure appropriate per la sicurezza, la protezione e il backup dei propri Contenuti. L'Amministrazione, inoltre, è responsabile di:

- Implementare il proprio sistema integrato di procedure, standard e policy di sicurezza e operative in base ai propri requisiti aziendali e di valutazione basati sul rischio
- Gestire i controlli di sicurezza dei dispositivi client in modo che dati o file siano soggetti a verifiche per accertare la presenza di virus o malware prima di importare o caricare i dati nei Servizi PSN
- Mantenere gli account gestiti in base alle proprie policy e best practice in materia di sicurezza
- Assicurare una adeguata configurazione e monitoraggio della sicurezza di rete

Assicurare il monitoraggio della sicurezza per ridurre il rischio di minacce in tempo reale e impedire l'accesso non autorizzato ai servizi PSN attivati dalle reti dell'Amministrazione, che deve includere sistemi anti-intrusione, controllo degli accessi, firewall e altri eventuali strumenti di gestione dalla stessa gestiti.

8. CONFIGURATORE

Di seguito, l'export del Configuratore contenente tutti i servizi della soluzione con la relativa sintesi economica in termini di canone annuo e UT. La durata contrattuale (prevista per un massimo di 10 anni) dei servizi contenuti nel presente progetto sarà declinata all'interno del contratto di utenza.

Codice Fiscale	4733471009
Regione Sanitaria	ASL Roma 5
Emesso da	CSO
Codice Documento	2023-0000004733471009-PPdF-P1R1
Versione	5

VERSIONE PROCESSATORE	5.1

SERVIZIO	QUANTITÀ	COSTO UNITARIO
Industry Standard		€ 324.243,96
Hybrid Cloud on PSN Site		€
SecurePublicCloud		€
Public Cloud PSN Managed		€
Servizi di Migrazione	€ 955.179,76	
Servizi Professionali	€ -	

VDC	NOME	SERVIZIO	TECNOLOGIA	DESCRIZIONE	QUANTITÀ	HA	GRUPPO	COSTO UNITARIO
VDC_a	IAAS16	IndustryS tandard	IaaSSharedHA	Pool Large	8	Primario		€ 37.904,5600
VDC_a	IAAS03	IndustryS tandard	IaaSStorageHA	Storage High Performance	40	Primario		€ 14.562,0000
VDC_a	IAAS07	IndustryS tandard	IaaSStorageHA	Storage HP Encrypted	41	Primario		€ 20.446,7000
VDC_a	IAAS04	IndustryS tandard	IaaSStorageHA	Storage Standard Performance	75			€ 14.961,0000
VDC_a	DP02	IndustryS tandard	DataProtection	Backup	423	Primario		€ 137.119,6800
VDC_a DR	DP03	IndustryS tandard	DataProtection	Golden copy	127	Secondario		€ 81.512,8600
VDC_a	HOUSING05	IndustryS tandard	Housing	IP Pubblici /29 (8 indirizzi)	2			€ 130,9000
VDC_a	HOUSING03	IndustryS tandard	Housing	Reseller connettività (fibra metropolitana)	2			€ 217,7800
VDC_a	CONN01	IndustryS tandard	Connettività	Connessione dedicata 1 Gbps	2			€ 17.388,4800

	SP 03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	136		€ 29.565,4400	
	SP 05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	77		€ 19.196,8700	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	46		€ 19.104,2600	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project Manager	99		€ 36.808,2000	
	SP 09	ServiziMigrazione	FiguraMigrazione	Business Analyst	31		€ 9.220,6400	
	SP 12	ServiziMigrazione	FiguraMigrazione	System and Network Administrator	44		€ 13.087,3600	
	SP 15	ServiziMigrazione	FiguraMigrazione	Junior Information Security Consultant	34		€ 10.112,9600	
	SP 22	ServiziMigrazione	FiguraMigrazione	Data Protection Specialist	73		€ 27.141,4000	
	SP 23	ServiziMigrazione	FiguraMigrazione	Systems Architect	57		€ 27.573,1800	
	SP 24	ServiziMigrazione	FiguraMigrazione	Product/Network/Technical Specialist	153		€ 51.258,0600	
	SP 01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	188		€ 72.821,8000	
	SP 04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	247		€ 77.891,4500	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project Manager	164		€ 60.975,2000	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	153		€ 38.144,4300	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	2		€ 930,6200	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	3		€ 747,9300	
	SP 04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	4		€ 1.261,4000	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	6		€ 1.495,8600	
	SP 03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	11		€ 2.310,4400	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project Manager	5		€ 1.859,0000	
	SP 01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	2		€ 774,7000	
	SP 04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	9		€ 2.838,1500	

	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	3		€ 747,9300	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	10		€ 2.493,1000	
	SP 03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing	12		€ 2.520,4800	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise	11		€ 4.568,4100	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project	3		€ 1.115,4000	
	SP 04	ServiziMigrazione	FiguraMigrazione	Cloud Application	13		€ 4.099,5500	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise	43		€ 17.858,3300	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	14		€ 3.490,3400	
	SP 01	ServiziMigrazione	FiguraMigrazione	Cloud Application	9		€ 3.486,1500	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	8		€ 1.994,4800	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project	24		€ 8.923,2000	
	SP 03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing	76		€ 15.963,0400	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise	5		€ 2.076,5500	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	3		€ 747,9300	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project	5		€ 1.859,0000	
	SP 01	ServiziMigrazione	FiguraMigrazione	Cloud Application	42		€ 16.268,7000	
	SP 02	ServiziMigrazione	FiguraMigrazione	Database Specialist and	80		€ 19.944,8000	
	SP 04	ServiziMigrazione	FiguraMigrazione	Cloud Application	92		€ 29.012,2000	
	SP 06	ServiziMigrazione	FiguraMigrazione	Enterprise	31		€ 12.874,6100	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project	64		€ 23.795,2000	
	SP 05	ServiziMigrazione	FiguraMigrazione	Cloud Security	30		€ 7.479,3000	
	SP 03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing	22		€ 4.620,8800	
	SP 07	ServiziMigrazione	FiguraMigrazione	Project	25		€ 9.295,0000	

	SP 07	Servizi Migrazione	FiguraMigrazione	Project Manager	25		€ 9.295,0000	
	SP 07	Servizi Migrazione	FiguraMigrazione	Project Manager	18		€ 6.692,4000	
	SP 07	Servizi Migrazione	FiguraMigrazione	Project Manager	34		€ 12.641,2000	
	SP 01	Servizi Migrazione	FiguraMigrazione	Cloud Application Architect	150		€ 58.102,5000	
	SP 01	Servizi Migrazione	FiguraMigrazione	Cloud Application Architect	269		€104.197,1500	
	SP 01	Servizi Migrazione	FiguraMigrazione	Cloud Application Architect	59		€ 22.853,6500	
	SP 07	Servizi Migrazione	FiguraMigrazione	Project Manager	135		€ 50.193,0000	

Tabella 18 - Configuratore

9 Rendicontazione

Di seguito, viene riportato un prospetto contenente la modalità di distribuzione dei servizi professionali, distinti per tipologia. I canoni dell'infrastruttura saranno attivati una volta resi disponibili i relativi servizi. La consuntivazione avverrà su base SAL mensili in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali

Servizi di Migrazione (Milestone Based)	Peso	Importo	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10
		€ 966.179,76										
Assess & Discovery	20%	286.953,93 €	114.921,57 €	172.032,36 €								
Setup	20%	191.036,95 €	19.103,69 €	95.517,84 €	76.414,84 €							
Migrazioni	45%	429.930,83 €			42.993,08 €	42.993,08 €	42.993,08 €	42.993,08 €	85.986,16 €	85.986,16 €	85.986,16 €	
Collaudo	5%	47.759,99 €									23.879,43 €	23.879,43 €
Totale Mensile			€ 133.725	€ 267.450	€ 119.337	€ 42.993	€ 42.993	€ 42.993	€ 85.966	€ 85.966	€ 109.846	€ 23.879
Totale		€ 966.179,76										

Tabella 19 - Rendicontazione

ALL 1

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.

CONTRATTO DI UTENZA

SOMMARIO

CONTRATTO DI UTENZA

<L'anno [•], il giorno [•] del mese di [•], ***da compilare a cura dell'Amministrazione***>

TRA

<[•] con sede in [•], [•] n. [•] codice fiscale [•], nella persona del [•] [•], in qualità di [•], nato a [•], il [•], C.F. [•] ("[•]" o "**Amministrazione Utente**") ***da compilare a cura dell'Amministrazione***>

E

La Società **Polo Strategico Nazionale S.p.A** ("**PSN S.p.A.**") con sede legale in Roma, via G. Puccini 6, numero di iscrizione nel Registro delle Imprese di Roma 1678264, Codice Fiscale e Partita IVA 16825251008 in persona del dott. [redacted] e domiciliato ai fini del presente contratto in via G. Puccini 6, nella qualità di Amministratore Delegato 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 Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri ("**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 <[•][•][•] ***da compilare a cura dell'Amministrazione>***, l'Amministrazione Utente presentava al Concessionario il proprio Piano dei Fabbisogni, così come definito all'art. 2, lett. zz. 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 <[•][•][•] ***da compilare a cura dell'Amministrazione>***, 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 <[•][•][•] ***da compilare a cura dell'Amministrazione>*** , il Concessionario ha presentato all'Amministrazione Utente il Piano di 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 ivi inclusa la comunicazione trasmessa al Concessionario, riguardante la richiesta di rilascio della garanzia definitiva, prevista all'art.26 della Convenzione, secondo lo schema standard messo a disposizione da parte del Concessionario ***[Nota: L'Amministrazione Utente per permettere al PSN di rilasciare la garanzia definitiva, preventivamente alla stipula, dovrà comunicare formalmente a PSN la richiesta di procedere con l'emissione della stessa, indicando l'importo da garantire e la durata. Per tale comunicazione PSN ha predisposto un testo standard di comunicazione che sarà trasmesso all'Amministrazione unitamente al Progetto del Piano dei fabbisogni. A seguito del rilascio della garanzia, PSN ne darà comunicazione all'Amministrazione tramite PEC].***

15. <L'Amministrazione Utente - in ottemperanza alla vigente normativa in materia di sicurezza sui luoghi di lavoro - ha predisposto il "Documento di valutazione dei rischi standard da interferenze", riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato il presente Contratto, indicando i costi relativi alla sicurezza. ***in ragione dei servizi da erogare, eventualmente da predisporre e produrre a cura dell'Amministrazione. Se non ricorre l'evenienza il punto 15 va cancellato sempre a cura Amministrazione>***

16. Il CIG del presente Contratto è il seguente: <[•]. ***da compilare a cura dell'Amministrazione>***

17. Il Codice univoco ufficio per Fatturazione è il seguente: <[•]. ***da compilare a cura dell'Amministrazione>***

18. Il CUP del presente Contratto è il seguente: <[•]. ***da compilare a cura dell'Amministrazione, se ne ricorre l'evenienza, in caso contrario il punto 18 va cancellato>***

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.

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 al successivo 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 ("**DEC**"), così come definito all'art. 2, lett. w. della Convenzione.

2. Il Responsabile Unico del Procedimento ("**RUP**") nominato dall'Amministrazione Utente è [•].

3. Entro 30 (trenta) giorni, le Parti istituiranno il Comitato di Contratto di Adesione ("Comitato"), presieduto dal Direttore del Servizio, a cui partecipano il RUP e il DEC dell'Amministrazione Utente, con il coinvolgimento dei referenti tecnici e delle figure di riferimento delle Parti. 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 Continuous Service Improvement.

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 del 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" alla Convenzione.

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" alla Convenzione.

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 d. lgs. n. 50/2016 e ss.mm.ii. (rubricato Codice dei contratti pubblici) ("**DLGS 50/2016**")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 n. 1000/00136942 presso Intesa San Paolo S.p.A., IBAN: IT13V0306901000100000136942 o, fermo il rispetto delle norme sulla tracciabilità dei flussi finanziari, su altro conto corrente intestato al Concessionario e previa indicazione di CIG e, qualora acquisito, di CUP nella causale di pagamento. I soggetti abilitati a operare sul conto sopra riportato per conto del Concessionario sono: l'Amministratore Delegato, dott. Emanuele Iannetti e il Chief Financial Officer, dott. Antonio Garelli.

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 **DLGS 50/2016**.

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 un 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" alla Convenzione.

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" alla Convenzione.

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 secondo lo schema tipo 1.2 del DM 19 gennaio 2018, n. 31 ("DM Garanzie"). Più in particolare, a garanzia delle obbligazioni contrattuali assunte nei confronti dell'Amministrazione Utente con la stipula del Contratto, il Concessionario presterà garanzia definitiva pari all'4% (quattro per cento) dell'importo del Contratto, salvo eventuali riduzioni di cui all'art. 103 del Codice intervenute prima o successivamente alla stipula. La garanzia sarà inviata dal Concessionario all'Amministrazione entro 30 giorni dalla stipula del presente contratto.

2. 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.

3. 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 d **DLGS 50/2016**. 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.

4. 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.

5. 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, 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) mancato reintegro della garanzia ove si verifichi la fattispecie di cui all'art. 15, commi 4 e 5 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 **DLGS 50/2016**, 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 **DLGS 50/2016**, 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.

5. Infine, l'Amministrazione Utente, decorsi 36 mesi dalla data di avvio della gestione del Servizio, potrà recedere dal presente Contratto nel caso in cui, durante la vigenza dello stesso, l'impegno di spesa presentato dall'Amministrazione Utente e necessario per la copertura degli esercizi successivi a quelli già deliberati alla data della firma del presente Contratto non sia approvato nello stanziamento all'interno del bilancio dell'Amministrazione Utente.

6. In tal caso l'Amministrazione Utente potrà recedere dal Contratto senza l'applicazione di penali e/o oneri aggiuntivi rispetto agli indennizzi e oneri derivanti dall'applicazione del precedente art. 20, comma 2, da lettera a) a d) inclusa, mediante comunicazione da inviarsi via Pec al PSN con almeno 120 giorni di preavviso rispetto al termine di cui sopra.

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 Roma, via G. Puccini 6, l'Amministrazione Utente elegge domicilio in <[•]. ***da compilare a cura dell'Amministrazione***>

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:

   per Polo Strategico Nazionale: convenzione.psn@pec.polostrategiconazionale.it

   per <[•]. ***da compilare a cura dell'Amministrazione***>

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 dell'Amministrazione Utente, che abbiano esercitato poteri autoritativi o negoziali per conto dell'Amministrazione Utente nei confronti del medesimo Concessionario, nel triennio successivo alla cessazione del rapporto di pubblico impiego.

2. <***da compilare a cura dell'Amministrazione*** [**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 alla Convenzione "Facsimile nomina Responsabile trattamento dei dati personali" secondo lo schema standard messo a disposizione da parte del Concessionario con i relativi sub-allegati che opportunamente compilato e firmato dall'Amministrazione Utente per accettazione della nomina dal Concessionario diventa parte integrante del presente Contratto.

Articolo 28
REGISTRAZIONE

1. La stipula del Contratto è soggetta a registrazione presso l'Agenzia delle Entrate. 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.

<[•] *Amministrazione, da compilare a cura dell'Amministrazione>*

<[•] *Ruolo, da compilare a cura dell'Amministrazione>*

<[•] *Firmatario, da compilare a cura dell'Amministrazione>*

Polo Strategico Nazionale S.p.A.

Amministratore Delegato

(Emanuele Iannetti)

ALL. 6.1

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 [●], la società Polo Strategico Nazionale S.p.A., meglio identificata nel Contratto d'utenza, (nel seguito "PSN" o il "Concessionario") è nominata 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 Concessionario/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 del trattamento 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 Concessionario/Responsabile del trattamento.

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 comuni (es. dati anagrafici e di contatto ecc.); ii) categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 c.d. sensibili; iii) dati personali relativi a condanne penali e reati di cui all'art. 10 del Regolamento UE 2016/679 c.d. giudiziari).

5. Le categorie di interessati sono: <**valorizzare in ragione del contratto** >.

6. Nel contesto della raccolta e della comunicazione dei dati personali degli interessati al PSN, l'Amministrazione è responsabile del corretto assolvimento degli obblighi che il Regolamento UE e, più in generale, la normativa applicabile in materia di protezione dei dati personali pone in capo ai titolari del trattamento. Il Titolare pertanto:

(i) garantisce che tutti i dati personali degli interessati siano o saranno lecitamente raccolti e comunicati al PSN;

(ii) garantisce che le istruzioni fornite al PSN siano lecite;

(ii) manleverà e terrà il PSN indenne da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione degli obblighi previsti dal Regolamento UE e dalla normativa applicabile in materia di protezione dei dati personali in capo al titolare.

7. Nell'esercizio delle proprie funzioni, il Concessionario/Responsabile del trattamento 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 del trattamento e di seguito indicate che il Concessionario/Responsabile del trattamento 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 2016/679 sulla protezione dei dati personali o delle altre disposizioni di legge relative alla protezione dei dati personali, il Concessionario/Responsabile 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: o si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza; o ricevano la formazione necessaria in materia di protezione dei dati personali; o trattino i dati personali osservando le istruzioni impartite dal Titolare al Concessionario/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 2016/679 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 2016/679 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 2016/679 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 del trattamento e dell'Autorità, laddove ne venga fatta richiesta>;

i) adottare le misure minime di sicurezza ICT per le PP.AA. **(specificare il livello richiesto)**, adeguate alla complessità del sistema informativo a cui si riferiscono e alla realtà organizzativa dell'Amministrazione utente **(come dettagliati all'interno del Manuale tecnico sulle misure di sicurezza "MTMS").**

8. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Concessionario/Responsabile 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 adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli

obblighi di cui all'art. 32 del Regolamento UE 2016/679. Tali misure comprendono tra le altre, se del caso **<personalizzare in ragione 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.

Tali misure sono state specificatamente inserite nel MTMS, allegato alla presente nomina di cui costituisce parte integrante. Il MTMS del PSN descrive i trattamenti, le responsabilità e le misure di sicurezza adottate dal PSN per garantire la sicurezza, in termini di Riservatezza, Integrità e Disponibilità, dei dati personali trattati nell'ambito dei Servizi di cui all'art. 5, comma 1 della Convenzione, che saranno offerti alle Pubbliche Amministrazioni coerentemente ai requisiti del contratto quadro ed alla documentazione di riscontro.

Questo documento, per ogni servizio commercializzato descrive in ottemperanza al Regolamento EU, l'elenco dei trattamenti con le relative responsabilità. Il documento verrà costantemente aggiornato e tali variazioni saranno adeguatamente comunicate alle Amministrazioni utenti.

Il MTMS, redatto secondo quanto previsto dal disciplinare di gara, è stato condiviso con il Concedente ed è disponibile, nell'ultima versione aggiornata (e nelle sue versioni storiche) nell'area riservata alle amministrazioni aderenti del portale della fornitura e comprende anche l'elenco dei sub Responsabili nominati dal Concessionario/Responsabile.

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.

9. Il Concessionario/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 2016/679, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, in loco o da remoto, 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 Concessionario/Responsabile del trattamento con un preavviso minimo di 15 giorni lavorativi dettagliando il perimetro dell'audit; 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 UE, o risulti che il Concessionario/Responsabile del trattamento agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il Concessionario/Responsabile del trattamento 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. Qualora l'Amministrazione utente dovesse esercitare il proprio diritto di ispezione e

verifica, dovrà sostenerne i relativi costi. Il PSN e i Soci si impegnano ad esporre costi ragionevoli.

10. Il Concessionario/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 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.

11. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Concessionario/Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Concessionario/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 adeguate 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 Concessionario/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 Concessionario/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 adeguate o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà concordato. 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.

12. Il Concessionario/Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati, salvo che ciò comporti uno sforzo sproporzionato. Qualora gli interessati esercitino tale diritto presso il Concessionario/Responsabile del trattamento, quest'ultimo è tenuto 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.

13. Il Concessionario/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 il alternativa**: Sub- Responsabile del trattamento si

impegna a supportare il Titolare nell'ambito di tale attività, salvo che ciò comporti uno sforzo sproporzionato.

14. Il Concessionario/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, a meno che non sia soggetto ad un obbligo di riservatezza; 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, salvo che ciò comporti uno sforzo sproporzionato.

15. Il Concessionario/Responsabile del trattamento deve comunicare al Titolare del trattamento 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.

16. Al termine della prestazione dei servizi oggetto del contratto, il Concessionario/Responsabile del trattamento, su indicazione del Titolare, si impegna a cancellare o restituire tutti i dati personali, ivi incluse le copie esistenti, dopo che è terminata la prestazione dei servizi, documentando per iscritto l'adempimento di tale operazione.

17. Il Concessionario/Responsabile del trattamento si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.

18. Il Concessionario/Responsabile del trattamento 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 Concessionario/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 Concessionario/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 Concessionario/Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni diretta responsabilità in relazione anche ad una sola comprovata 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.

Per accettazione della nomina

Roma, xx/yy/xxxx

Polo Strategico Nazionale S.p.A.

_____

ALL 6.2

Polo Strategico Nazionale

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

Manuale tecnico sulle misure di sicurezza "MTMS"

Data: 24/04/2023

Ed. 1 - ver. 01

PSN-MTMS_v1.docx

QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
PIANO OPERATIVO			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	01	24/04/2023	Prima emissione

NUMERO TOTALE PAGINE:	118

AUTORE	
Team di lavoro PSN	Unità operativa Risk & Compliance, Solution, Technology & Officer, Security & Information e con il supporto di tutte le funzioni interne coinvolte nel processo e Fornitori Soci

REVISIONE	
Referente del Servizio	Paolo Trevisan

APPROVAZIONE	
Direttore del Servizio	Antonio Garelli

LISTA DI DISTRIBUZIONE

INTERNA A:

- HR & Organization Officer
- Procurement Officer
- Communication Officer
- Legal Officer
- Financial Officer
- Marketing & Sales Office
- Solution Officer
- Risk & Compliance Officer
- Technology & Officer
- Security & Information Officer

ESTERNA A:

- Direttore dell'Esecuzione Contrattuale PSN
- Pubbliche Amministrazioni aderenti a PSN
- Soci gestori (TIM, Leonardo, Sogei)
- Subfornitori, subappaltatori (per quanto applicabile)

Polo Strategico Nazionale

INDICE

1 EXECUTIVE SUMMARY

1.1 Scopo del documento

Il **Manuale tecnico sulle misure di sicurezza** (nel seguito "**MTMS**") **della società Polo Strategico Nazionale S.p.A.** ("**PSN**") descrive i trattamenti, le responsabilità e le misure di sicurezza adottate dal PSN per garantire la sicurezza del dato, in termini di Riservatezza, Integrità e Disponibilità.

Questo documento, per ogni servizio commercializzato in ambito descrive in ottemperanza al GDPR (REGOLAMENTO EU N. 679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI) l'elenco dei trattamenti con le relative responsabilità, le misure di sicurezza di cui all'art. 32 GDPR ovvero le misure tecniche organizzative indicate nelle Determinazioni ACN N. 306 e 307 /2022 in funzione della classificazione dei dati gestiti dalla PA, secondo la metrica di ACN (dato ordinario, critico e strategico).

L'esecuzione dei trattamenti, secondo l'art. 28 del GDPR, deve essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il Responsabile al Titolare (ed al rispetto delle istruzioni impartite). Nella fattispecie PSN S.p.A. utilizzerà l'Allegato E - Facsimile Nomina Responsabile del Trattamento dei dati personali della Convenzione stipulata fra PSN S.p.A. e DTD e il presente documento richiamato nell'Allegato E, per procedere alla nomina di un altro Responsabile del trattamento (di seguito "Sub-Responsabile del trattamento").

2 RIFERIMENTI

In questo capitolo si riporta un elenco delle principali fonti normative e dei documenti applicabili e di riferimento per il presente documento.

2.1 Normative di riferimento

[1] 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*);

[2] Provvedimento "Amministratori di sistema" del 27 novembre 2008 e successiva modifica del 25 giugno 2009

[3] PSNC **(Perimetro di Sicurezza Nazionale Cibernetica)** Decreto-legge 105/2019 (convertito con modificazione dalla Legge 18 novembre 2019, n. 133) - 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

[4] Misure minime di sicurezza informatica per la PA (AgID GG.UU 4/2017)

[5] Framework Nazionale di Cyber Security e Data Protection 2.0

[6] Determinazione AgID n. 628/2021 e Determinazioni ACN 306/2022 e 307/2022 e relativi allegati

3 DEFINIZIONI E ACRONIMI

All'interno del documento si fa riferimento **alle definizioni** riportate nella tabella che segue.

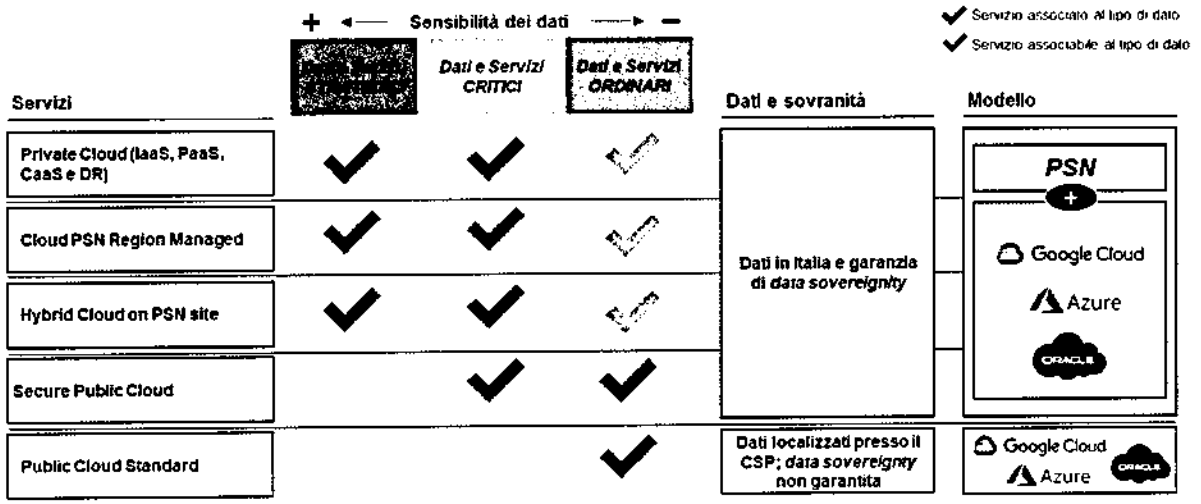
Glossario	Descrizione
PA	Pubbliche Amministrazioni
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
MTMS	Manuale tecnico sulle misure di sicurezza
Dati personali	Qualsiasi informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica e che possa fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, etc
GDPR	*Il General Data Protection Regulation* è il 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
Normativa Privacy Applicabile	Il 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 ("GDPR") e le leggi nazionali tra cui il D. Lgs. 196/2003 e s.m.i (Codice della privacy), il D.lgs n. 101/2018 che specificano ulteriormente l'applicazione delle norme contenute nel GDPR, i provvedimenti del Garante Privacy, le Linee Guida *dell'European Data Protection Board* nonché gli orientamenti della giurisprudenza.
Responsabile ex art 28 GDPR	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che non opera sotto l'autorità o il diretto controllo del Titolare e, singolarmente o insieme ad altri, in virtù di apposito contratto di servizio o altro atto scritto equivalente, tratta i Dati Personali per conto del Titolare.
Titolare	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

4 AMBITO DI APPLICABILITA'

Il presente MTMS si applica a tutti i servizi previsti dal PSN e contrattualizzati dalla PA.

L'offerta del PSN è ampia e flessibile e permetterà alle PA di scegliere i servizi più idonei alle loro necessità, in base ai diversi modelli offerti. In particolare, il PSN offre soluzioni Cloud specifiche, sviluppate anche tramite specifici accordi industriali con CSP leader di mercato, tramite le quali è possibile offrire tutti servizi cloud richiesti, ma progettati specificamente per assicurare autonomia tecnologica, controllo diretto sul dato, cyber-resilienza, conformità ai requisiti di classificazione del dato (allineamento alle direttive ACN).

Tramite il PSN la PA potrà scegliere le soluzioni cloud più adatte a garantire innovazione ma anche privacy, sicurezza, compliance, efficienza e sovranità del dato come si evince dalla seguente figura:



Caratteristiche dei servizi cloud offerti alle PA

5 ANAGRAFICA FORNITORI DEL PSN

In questo capitolo sono elencati tutti i Fornitori che nei servizi di seguito dettagliati possono intervenire come responsabile esterno del trattamento:

TIM S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

Leonardo S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

Sogei S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

6 DESCRIZIONE DEI MACRO-TRATTAMENTI

In questo capitolo sono descritti i macro-trattamenti riportati nei capitoli dei servizi, successivamente descritti:

Macro-Trattamenti	Descrizione	Possibili operazioni di trattamento dati personali associate alla categoria
Gestione delle infrastrutture e Service Management	Si intendono i servizi base di gestione delle infrastrutture necessarie all'erogazione del Servizio e i servizi di gestione al Cliente	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Trattamenti inerenti la Cybersecurity	Si intendono tutte le attività riferite alle attività di Security Operation tra cui anche la raccolta ed analisi dei log (es. FW, IDS, SIEM,..) ai fini dell'erogazione dei servizi di Cybersecurity (es. SOC);	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Supporto al Cliente per la migrazione e gestione.	Si intendono tutte le attività a corredo che il Cliente potrebbe chiedere come servizi professionali per gestire il suo contesto e per supportarlo durante il processo di migrazione di re-architect e di re-platform. Possono comportare attività di gestione sistemistica, middleware, applicativa. Compresi i servizi professionali di sicurezza.	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Erogazione al Cliente dei servizi di formazione	Si intendono tutte le attività a supporto del Cliente relativamente a Erogazione al Cliente dei servizi di formazione.	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione

6.1 Macro-Trattamenti associati ai servizi dei Soci

Nella tabella a seguire viene descritta l'associazione tra i macro-trattamenti prima descritti ed i servizi erogati dai Soci:

Servizio Soci	TIM	LDO	SOGEI	Macro-Trattamenti
Spazi attrezzati	X	-	-	Gestione delle infrastrutture e Service Management
Connettività	X	-	-	Gestione delle infrastrutture e Service Management
COPS - servizi di gestione cliente (Help Desk di primo livello)	X	-	-	Gestione delle infrastrutture e Service Management
SERVICE MANAGEMENT - servizio di gestione del cliente	X	X	-	Gestione delle infrastrutture e Service Management
Business & Culture enablement	-	-	X	Erogazione al Cliente dei servizi di formazione
Sicurezza - Servizio CERT	-	X	-	Trattamenti inerenti la Cybersecurity
Security Operations	-	X	-	Trattamenti inerenti la Cybersecurity
Servizi professionali di sicurezza	X	X	-	Supporto al Cliente per la migrazione e gestione.
Paas Industry	-	X	-	Gestione delle infrastrutture e Service Management
Secure Public Cloud quota PSN	X	X	-	Gestione delle infrastrutture e Service Management
Public Cloud a PSN Managed	X	X	-	Gestione delle infrastrutture e Service Management
Hybrid Cloud on PSN site	-	X	-	Gestione delle infrastrutture e Service Management
IT Infrastructure - Controllo produzione	X	-	-	Gestione delle infrastrutture e Service Management
IT Infrastructure - Service Operations	X	X	X	Supporto al Cliente per la migrazione e gestione.
Servizio di migrazione	X	X	X	Supporto al Cliente per la migrazione e gestione.
Intra Migrazione	X	X	X	Supporto al Cliente per la migrazione e gestione.
Re-platform	X	X	X	Supporto al Cliente per la migrazione e gestione.
Re-architect	X	X	X	Supporto al Cliente per la migrazione e gestione.

7 SERVIZIO HOUSING

Il Servizio Infrastrutturale in modalità Housing Dedicato consiste nella messa a disposizione, da parte del 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.

7.1 Tipo dato - Trattamento e Responsabile del Trattamento

Per questo servizio è previsto il solo trattamento, da parte di PSN e TIM, di conservazione fisica dei dati personali nei Data Center dedicato al PSN.

8 SERVIZIO HOSTING

Il Servizio Industry Standard Hosting consiste nel rendere disponibile alle PPAA una infrastruttura fisica e dedicata.
Le modalità di erogazione sono:

- Hosting su rack condivisi: le PPAA avranno accesso a porzioni dedicate di rack condivisi con altre PPAA
- Hosting su rack dedicati: le PPAA avranno accesso a rack esclusivi/segregate

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

8.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categorie Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

9 IAAS INDUSTRY STANDARD (Private, Shared, Storage)

Il Polo Strategico Nazionale ha una propria Cloud Platform con la quale erogare servizi IaaS ai clienti finali. La Cloud Platform è concepita nativamente in High Availability tra almeno 2 DC (HA-Zone) costituenti una specifica Region e in particolare 2 Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA Zone di ogni Region e le stesse Region sono interconnesse da un unico SDN Network layer in grado di consentire un modello di architettura flat che garantisca workload mobility e alta affidabilità intrinseca delle soluzioni Cloud.

L'infrastruttura, è 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. TIM disponendo di questi diversi DC sul territorio nazionale atti all'erogazione di servizi IT, ne ha prescelti 4 in particolare per l'erogazione dei servizi Cloud PSN.

Questi DC sono:

- ***Region Nord***:
  - *Rozzano*
  - *Santo Stefano Ticino*

- ***Region Centro/Sud***:
  - *Acilia*
  - *Pomezia*

Il servizio IaaS Private garantisce delle risorse elaborative in uso esclusivo al cliente finale e tali risorse sono individuate attraverso Pool di Risorse che comprendono vCPU, vRAM e Storage Space e che in particolare indirizzano interi Bare Metal Hypervisors server come elementi minimi di configurazione. Quindi, è evidente che questo Cloud Service prevede risorse completamente dedicate e riservate ad un unico e solo cliente finale. Grazie alla disponibilità di questo Pool di Risorse, il cliente finale potrà autonomamente creare e gestire VMs e relativo vNetworking per consentire l'erogazione di un determinato modello di servizio applicativo installato all'interno delle VM sempre in modo del tutto autonomo. I Pool di Risorse possono essere allocati in modalità "Local Only" in una specifica HA Zone oppure in modalità "Stretched" e quindi con span in due HA Zone di una stessa Cloud Region.

Il PSN è responsabile della gestione completa dell'infrastruttura sottesa, e rende disponibile gli strumenti e le console per la gestione in autonomia degli ambienti virtuali contrattualizzati.

Il servizio IaaS Shared garantisce delle risorse elaborative al cliente finale e tali risorse sono individuate attraverso dei Pool di Risorse "elastiche" che comprendono vCPU, vRAM e Storage Space. Le risorse sono definite elastiche perchè i Pool possono essere scelti in differenti sizing in funzione delle esigenze e, una volta allocati, possono essere pur sempre oggetto di resizing. Grazie alla disponibilità di questo Pool di Risorse, il cliente finale potrà autonomamente creare e gestire VMs e relativo vNetworking per consentire l'erogazione di un determinato modello di servizio applicativo installato all'interno delle VM sempre in modo del tutto autonomo.

Le risorse elaborative incluse nel Pool di Risorse sono ricavate su Bare Metal Hypervisors server condivisi con altri Pool di Risorse di altri clienti ma ad ogni modo ogni cliente avrà una netta separazione logica rispetto al contesto/workload di ogni altro cliente. I Pool di Risorse possono essere allocati in modalità "Local Only" in una specifica HA Zone oppure in modalità "Stretched" e quindi con span in due HA Zone. All'interno del proprio contesto, il cliente finale disporrà anche di un Catalogo di VM template da poter utilizzare per avviare appunto istanze di VM nelle proprie risorse elaborative disponibili. Il Catalogo conterrà VM template generati dal PSN come fornitore del servizio ma potrà anche avere una sezione privata e quindi gestita autonomamente dal cliente finale per la registrazione di VM template "proprietari" da poter mettere a disposizione dei propri utenti finali.

Il PSN è responsabile della gestione completa dell'infrastruttura sottesa, comprensiva degli strumenti di automation e orchestration.

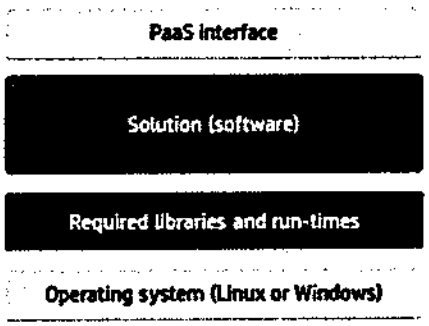
9.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10 SERVIZI PaaS

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



Componenti Servizio PaaS Industry

In particolare, questi componenti consisteranno in:

- 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.

Il PSN è responsabile dell'infrastruttura sottostante comprensiva degli strumenti di automation e orchestration e si compone dei sottoservizi nei seguenti paragrafi

10.1 PaaS DB

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:

- 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.

10.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10.2 PaaS (Spid Enabling & Profiling)

In aggiunta ai servizi di Identity and Access Management che garantiscono i diritti di accesso alle componenti tecniche in ambito PSN (IaaS, PaaS, console unica di gestione, ecc.), viene reso disponibile dal 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 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 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.

10.2.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Gestione delle infrastrutture e Service Management	PSN, TIM, /Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

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

10.3.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10.4 PaaS AI (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.
- **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 onitoraggio 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:** questa piattaforma PaaS pronta all'uso è 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.

10.4.1 Tipo dato - Trattamento e Responsabile del Trattamento

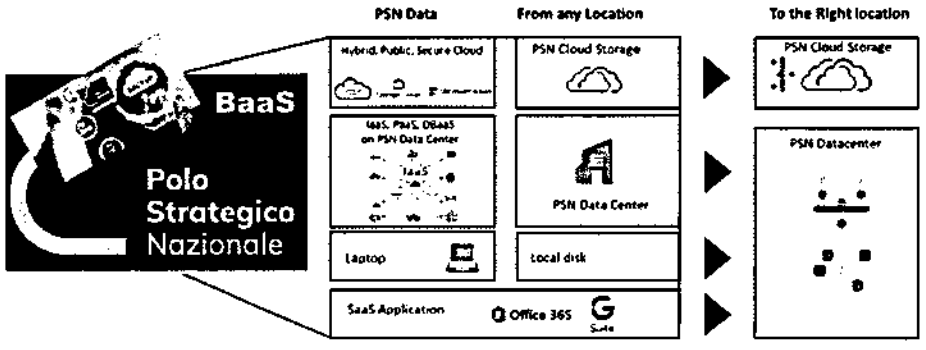
Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

11 DATA PROTECTION (Opzione DR, BackUp, Golden Copy)

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, PSN mette a disposizione un **servizio opzionale** aggiuntivo che analizza i backup mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione. Tale funzionalità 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.

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.

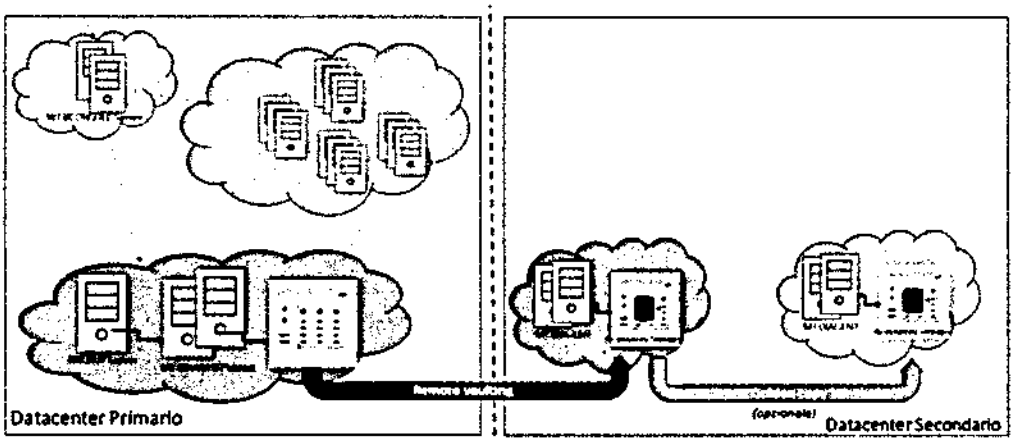
Tale servizio BaaS è erogato attraverso una console centralizzata attraverso la quale, in modalità self-managed, è possibile gestire la protezione dei vari contesti da proteggere (Files, VM, Container (k8), tutti i principali database come SAP-HANA, Exchange, SQL, Oracle, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, o i principali PaaS). Il servizio 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.
Per tutti i backup sarà possibile effettuare una ulteriore copia secondaria al completamento della copia primaria.



Modalità di Erogazione Servizio BaaS: Golden Copy

L'utente dopo aver inserito le sue credenziali per accedere al portale BaaS potrà schedulare i job di backup sia su base giornaliera che su base settimanale attivare manualmente (on demand) la partenza del job di backup in funzione delle proprie esigenze.

Naturalmente, per ogni singolo sistema configurato sul servizio BaaS è possibile scegliere i dati (file, cartelle, VM, ecc.) che dovranno essere protetti, le modalità di backup (full o incrementale) e la retention da applicare.
Analogamente, per quanto riguarda il ripristino dei dati, l'utente, collegandosi al portale del servizio, può selezionare singoli file o interi set di backup (insieme di cartelle e file) tra quelli disponibili nel sistema scegliendo l'opportuna data di ripristino dei dati. Contestualmente, alla configurazione dei suoi backup, l'utente può scegliere di effettuare una copia secondaria dei dati di backup:



Esecuzione Copia di Back-up

Il Disaster Recovery "as-a-Service" (DRaaS) è invece 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. Il DRaaS si
basa sulla replica e sull'hosting dei server in un site del PSN diverso rispetto all'ubicazione primaria

11.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

12 CaaS

12.1 Servizio CaaS

Il Servizio Infrastrutturale in modalità CaaS consiste nella messa a disposizione, da parte del PSN, di una infrastruttura in grado di distribuire e gestire tutte le applicazioni basate su container in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera.

Il servizio offerto si basa sul progetto **Open Source OKD**, 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.

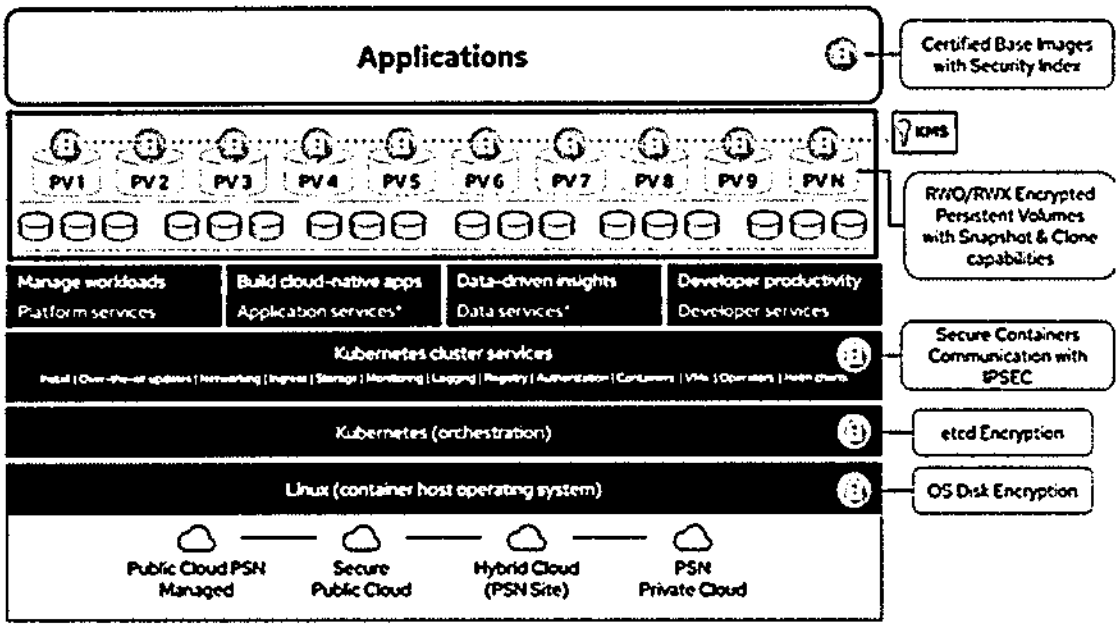
In particolare, per l'erogazione del servizio sarà utilizzata la distribuzione Red Hat di OpenShift, di cui OKD è il corrispondente progetto parallelo di community, su cui è basata appunto questa distribuzione: come per tutte le distribuzioni Red Hat, sul portale di accesso (access.redhat.com) è sempre 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.



Architettura OCI

12.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

13 SERVIZI CSP

13.1 Public Cloud PSN Managed

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.

Tale servizio permetterà alle Amministrazione di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica e gestione operata da personale PSN. Le caratteristiche salienti del Public Cloud PSN Managed sono:

- Residenza dei dati in Italia.
- Controllo operativo affidato al Managed Service Provider (MSP), nel caso specifico TIM.
- Localizzazione nei Data Center del CSP, ma con segregazione fisica degli apparati dalle Region Pubbliche-
- Control Plane locale e disconnesso dal CSP-
- BYOID, ovvero liberta' di scegliere un sistema di identity proprietario.
- Ampia compatibilita' e offerta di servizi basati su Open-Source Software (OSS).
- Nessun accesso diretto del CSP all'infrastruttura o al software.
- Connettivita' verso l'esterno integralmente gestita da personale TIM o PSN
- Utilizzo dei servizi di sicurezza forniti da Google, ma gestiti da TIM.
- Ampio supporto dei servizi CSP tra cui AI/ML, Data Analytics, servizi di containerizzazione e servizi forniti da terze parti
- Gestione mediante strumenti e servizi basati su uno stack OSS, con API aperte e strumenti che assicurano semplicità, coerenza e portabilità in linea con i principi di Cloud Switching della recente proposta dell'EU Data Act.
- Gestione di tutta la Supply chain, dal rilascio del software, alla gestione dell'hardware

13.1.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Google)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Google ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

13.1.2 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Oracle)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Oracle ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

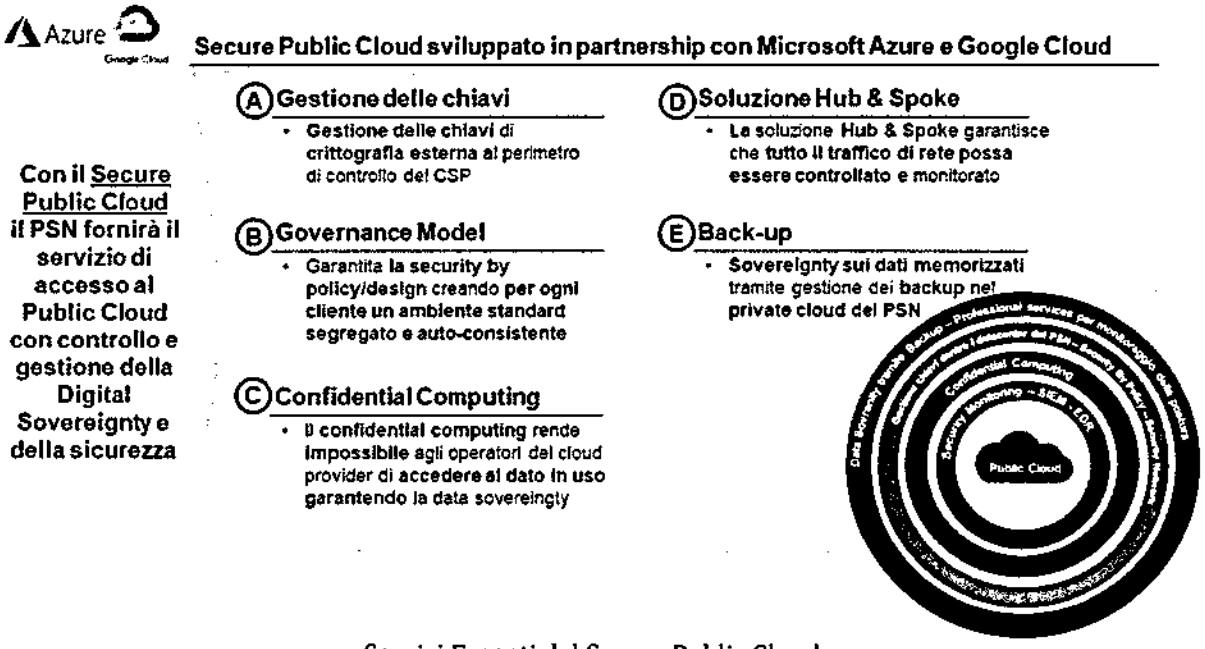
13.2 Secure Public Cloud

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;
- **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).

Di seguito, sono indicati i servizi di base erogati dal SPC per le pubbliche amministrazioni aderenti:



Servizi Erogati dal Secure Public Cloud

13.2.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Google)

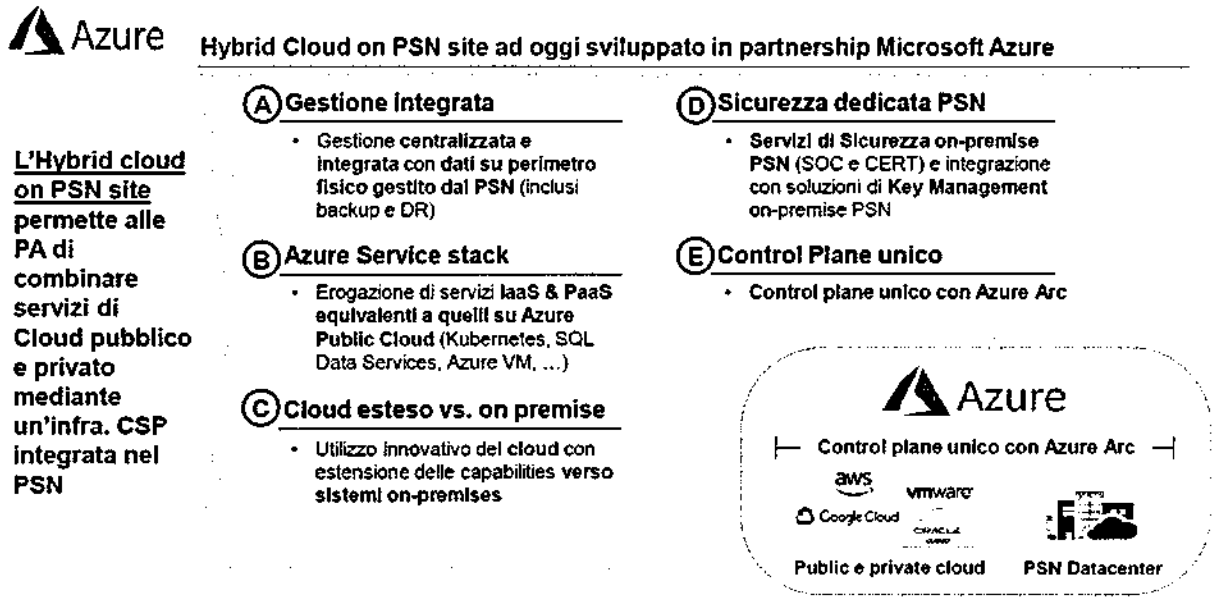
Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Google ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Google ed eventuali Subresponsabili

13.2.2 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Microsoft)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Microsoft ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Microsoft ed eventuali Subresponsabili

13.3 Hybrid Cloud on PSN Site

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



Servizi Erogati dall'Hybrid Cloud on PSN

Il servizio mette a disposizione infrastrutture iperconvergenti dedicate:

- Basate su **soluzioni HCI** (Hyperconverged Infrastructure) **dedicate** a ciascun cliente e **ubicate all'interno** dei Data Center del **PSN**;
- 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.;
- 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.

13.3.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Microsoft)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Microsoft ed eventuali subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Microsoft ed eventuali Subresponsabili

14 SERVIZI DI MIGRAZIONE, EVOLUZIONE E PROFESSIONAL SERVICES

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

14.1 Tipo dato - Trattamento e Responsabile del Trattamento

Potrebbero essere svolti trattamenti di Dati Personali e Personali Particolari, nell'erogazione dei servizi professionali.

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)		
	Supporto al Cliente per i servizi di migrazione, di re-architect e di re-platform e di gestione	PSN, TIM, Leonardo, Sogei e loro eventuali Sub-Responsabili

15 BUSINESS & CULTURE ENABLEMENT

La trasformazione digitale deve essere accompagnata non solo da un'innovazione tecnologica, ma soprattutto da un cambiamento delle metodologie di lavoro e dall'organizzazione dello stesso. Cambiare la cultura delle amministrazioni aderenti vuol dire agire sulla leadership e sulla collaborazione tra le persone.
Disegnare e produrre servizi e prodotti digitali per il bacino di utenza delle Amministrazioni aderenti, significa anche adottare modelli di lavoro omogenei; l'attenzione alla user experience consente infatti di rendere questa cultura una prassi da applicare sia all'interno dell'Amministrazione che verso gli utenti finali.
Punti nodali di questa trasformazione sono il change management ed il modello formativo. Per questi motivi, il 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;
- Competenze e modello manageriale;
- Tool Collaborativi;
- Employee experience;
- Modello di innovazione.

Inoltre, sarà disponibile 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;
- ulteriore formazione trasversale con corsi specifici definiti a catalogo e/o customizzati su esigenze dell'Amministrazione.

In base alle necessità delle singole amministrazioni aderenti sarà individuato il mix di figure professionali necessarie, tra quelle messe a disposizione dal PSN, che effettuerà le attività richieste.

15.1 Tipo dato - Trattamento e Responsabile del Trattamento

Sono previsti trattamenti di raccolta e conservazione di Dati Personali Comuni per i quali verranno garantite le istruzioni presenti nella lettera di nomina (Allegato E).

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Erogazione al Cliente dei servizi di formazione	PSN, Sogei ed eventuali Subresponsabili

16 ALLEGATO - Misure di sicurezza e compliance

In questo capitolo sono elencate le misure definite by design e by default che, come da Art.32 del GDPR, garantiscono un livello di sicurezza adeguato al rischio dei servizi in ambito.

16.1 Misure derivanti dal provvedimento del Garante Privacy del 27/11/2008 in tema "Amministratori di Sistema"

Requisito
L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

16.2 Determinazioni AgID e ACN – Misure di sicurezza per qualificazione infrastrutture/servizi per la PA

Le misure di sicurezza per la qualificazione delle Infrastrutture e dei servizi per la PA secondo la determinazione AgID (**Determinazione n. 628/2021**) e ACN (**Determinazioni 306/2022 e 307/2022** e relativi allegati), sono soddisfatte dalle certificazioni come da tabella:

QUALIFICA AGID - Circolari AGID n.2 e n.3 del 2018

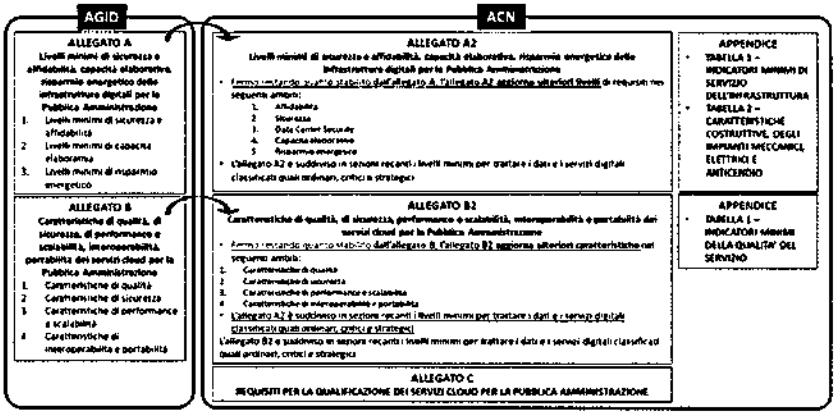
- Definizione tipologia di qualifica: qualifica di «tipo C» → CSP / qualifica di «tipo A» → servizi IaaS/PaaS / qualifica di «tipo B» → servizi SaaS

REQUISITI PER LA QUALIFICAZIONE SERVIZI CLOUD PER LA PA – DIC. 2021/GEN. 2022

Criteri definiti da AGID e Agenzia Nazionale per la Cybersicurezza (ACN), d'intesa con il Dipartimento per la Trasformazione Digitale (DTD)*

Tipologia dati	Requisiti per qualificazione servizi cloud PA		Requisiti per qualificazione infrastrutture	
	Qualificazione prevista	Certificazioni richieste	Qualificazione prevista	Certificazioni richieste
Ordinari	Livello 1 (QC1)	È richiesto il conseguimento delle seguenti certificazioni: - ISO 9001 - ISO 27001 - ISO 27017 e 27018 (o in alternativa CSA STAR LEVEL 2)	Livello 1 (QI1)	- Conseguimento della certificazione ISO 9001 - Autocertificazione che attesti conformità a standard ISO 27001
	Livello 2 (QC2)	In aggiunta a quanto già previsto per QC1, è richiesta: - Autocertificazione che attesti conformità a standard ISO 22301 e ISO 20000	Livello 2 (QI2)	In aggiunta a quanto già previsto per QI1, è richiesta: - Autocertificazione che attesti conformità a standard ISO 22301 - Conseguimento della certificazione ISO 27001
Strategici	Livello 3 (QC3)	In aggiunta a quanto già previsto per QC2, è richiesto il conseguimento delle seguenti certificazioni: - ISO 22301 - ISO 20000-1 - CSA - STAR Level 2	Livello 3 (QI3)	In aggiunta a quanto già previsto per QI2, è richiesto il conseguimento delle seguenti certificazioni: - ISO 22301
	Livello 4 (QC4)	In aggiunta a quanto già previsto per QC3, non sono richieste ulteriori certificazioni, ma solo il rispetto di requisiti specifici.	Livello 4 (QI4)	In aggiunta a quanto già previsto per QI3, non sono richieste ulteriori certificazioni, ma solo il rispetto di requisiti specifici.

Nei seguenti paragrafi sono riportate le misure di sicurezza di dettaglio organizzate come da figura allegata:



16.2.1 Requisiti AgID Allegato A

ID Requisito	Specifica Requisito
IN-CE-01	L'Amministrazione che eroga servizi ad altre amministrazioni deve formalizzare e pubblicare le informazioni relative ai servizi tramite il CED ricorrendo ad un apposito catalogo servizi, in conformità alle best practice ITIL. Il catalogo deve essere gestito e manutenuto attraverso un processo aderente alle best practice sul service catalogue management ITIL o alle linee guida riportate dallo standard ISO/IEC 20000-2.
IN-CE-02	L'Amministrazione che eroga servizi ad altre amministrazioni deve rendere nota la capacità di elaborazione totale del CED, quella occupata, quella libera per soddisfare i propri piani di capacity e quella a disposizione di Amministrazioni ospitate. Nello specifico, per ciascuna misura, l'Amministrazione deve dichiarare: - la superficie della sala CED o l'equivalente in numero di rack o di unità rack (U); - il numero e la tipologia di server fisici o di server farm disponibili, fornendo la capacità computazionale totale ottenuta come somma di memoria RAM disponibile [in GB], somma di CPU/Core e vCore, MIPs per gli apparati Mainframe, storage [in TB].
IN-RE-01	L'Amministrazione deve determinare con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti 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 per gli apparati.
IN-RE-02	L'Amministrazione deve avere adottato formalmente procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)
IN-SA-DC-08-01	L'Amministrazione deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.
IN-CE-03	La capacità elaborativa del CED deve essere gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000- 2.
IN-SA-DC-01-01	L'Amministrazione garantisce il presidio operativo del Data Center 24/7/365.
IN-SA-DC-02-01	L'Amministrazione deve dimostrare che gli immobili in cui sono situati i Data Center devono essere nella disponibilità esclusiva dell'Ente sulla base di uno dei seguenti titoli di possesso: 1. Proprietà; 2. locazione/comodato da altra PA o Demanio; 3. leasing immobiliare con possibilità di riscatto; 4. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".
IN-SA-DC-03-01	Il Data Center deve essere stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.

ID Requisito	Specifica Requisito
IN-SA-DC-04-01	Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
IN-SA-DC-05-01	L'indice di disponibilità del singolo Data Center deve essere almeno pari al 99,98 % (come rapporto tra le ore totali di servizio del Data center e le ore di disponibilità del Data center) al netto dei fermi programmati e almeno pari al 99,6% comprendendo i fermi programmati.
IN-SA-DC-06-01	L'Amministrazione deve garantire le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
IN-SA-DC-07-01	L'Amministrazione deve garantire che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
IN-SA-DE.CM-1-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-4-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-7-01	L'Amministrazione implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
IN-SA-DE.CM-8-01	L'Amministrazione implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)
IN-SA-ID.AM-1-01	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FNCS (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
IN-SA-ID.AM-2-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
IN-SA-ID.AM-3-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
IN-SA-ID.AM-6-01	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FNCS. (Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner))
IN-SA-ID.GV-1-01	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)

ID Requisito	Specifica Requisito
IN-SA-ID.RA-5-01	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
IN-SA-PR.AC-1-01	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
IN-SA-PR.AC-2-01	L'Amministrazione implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
IN-SA-PR.AC-3-01	L'Amministrazione implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
IN-SA-PR.AC-4-01	L'Amministrazione implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
IN-SA-PR.AT-1-01	L'Amministrazione implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
IN-SA-PR.AT-2-01	L'Amministrazione implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
IN-SA-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
IN-SA-PR.DS-5-01	L'Amministrazione implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))
IN-SA-PR.DS-6-01	L'Amministrazione implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
IN-SA-PR.IP-1-01	L'Amministrazione implementa la sotto-categoria PR.IP-1 del FNCS. (Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. Principio di minima funzionalità))

ID Requisito	Specifica Requisito
IN-SA-PR.IP-12-01	L'Amministrazione implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
IN-SA-PR.IP-4-01	L'Amministrazione implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
IN-SA-PR.IP-9-01	L'Amministrazione implementa la sotto-categoria PR.IP-9 del FNCS. E' stato predisposto il piano di Disaster recovery. Sono state adottate formali procedure di emergenza in caso di indisponibilità parziale dei servizi. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
IN-SA-PR.MA-1-01	L'Amministrazione implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)
IN-SA-PR.MA-2-01	L'Amministrazione implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati)
IN-SA-RC.RP-1-01	L'Amministrazione implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
IN-SA-RS.MI-3-01	L'Amministrazione implementa la sotto-categoria RS.MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)

16.2.2 Requisiti AgID Allegato B

ID Requisito	Specifica Requisito
IN-CE-01	L'Amministrazione che eroga servizi ad altre amministrazioni deve formalizzare e pubblicare le informazioni relative ai servizi tramite il CED ricorrendo ad un apposito catalogo servizi, in conformità alle best practice ITIL. Il catalogo deve essere gestito e manutenuto attraverso un processo aderente alle best practice sul service catalogue management ITIL o alle linee guida riportate dallo standard ISO/IEC 20000-2.
IN-CE-02	L'Amministrazione che eroga servizi ad altre amministrazioni deve rendere nota la capacità di elaborazione totale del CED, quella occupata, quella libera per soddisfare i propri piani di capacity e quella a disposizione di Amministrazioni ospitate. Nello specifico, per ciascuna misura, l'Amministrazione deve dichiarare: - la superficie della sala CED o l'equivalente in numero di rack o di unità rack (U); - il numero e la tipologia di server fisici o di server farm disponibili, fornendo la capacità computazionale totale ottenuta come somma di memoria RAM disponibile (in GB), somma di CPU/Core e vCore, MIPs per gli apparati Mainframe, storage (in TB).
IN-RE-01	L'Amministrazione deve determinare con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti 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 per gli apparati.
IN-RE-02	L'Amministrazione deve avere adottato formalmente procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)
IN-SA-DC-08-01	L'Amministrazione deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.
IN-CE-03	La capacità elaborativa del CED deve essere gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.
IN-SA-DC-01-01	L'Amministrazione garantisce il presidio operativo del Data Center 24/7/365.
IN-SA-DC-02-01	L'Amministrazione deve dimostrare che gli immobili in cui sono situati i Data Center devono essere nella disponibilità esclusiva dell'Ente sulla base di uno dei seguenti titoli di possesso: 1. Proprietà; 2. locazione/comodato da altra PA o Demanio; 3. leasing immobiliare con possibilità di riscatto; 4. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".
IN-SA-DC-03-01	Il Data Center deve essere stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.
IN-SA-DC-04-01	Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
IN-SA-DC-05-01	L'indice di disponibilità del singolo Data Center deve essere almeno pari al 99,98 % (come rapporto tra le ore totali di servizio del Data center e le ore di disponibilità del Data center) al netto dei fermi programmati e almeno pari al 99,6% comprendendo i fermi programmati.
IN-SA-DC-06-01	L'Amministrazione deve garantire le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
IN-SA-DC-07-01	L'Amministrazione deve garantire che tutti i server del Data Center sono connessi ad apparati per la continuità elettrica (UPS).
IN-SA-DE.CM-1-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-4-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-7-01	L'Amministrazione implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
IN-SA-DE.CM-8-01	L'Amministrazione implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)

IN-SA-ID.AM-1-01	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FNCS (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
IN-SA-ID.AM-2-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
IN-SA-ID.AM-3-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
IN-SA-ID.AM-6-01	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FNCS. (Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner))
IN-SA-ID.GV-1-01	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)
IN-SA-ID.RA-5-01	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
IN-SA-PR.AC-1-01	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
IN-SA-PR.AC-2-01	L'Amministrazione implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
IN-SA-PR.AC-3-01	L'Amministrazione implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
IN-SA-PR.AC-4-01	L'Amministrazione implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
IN-SA-PR.AT-1-01	L'Amministrazione implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
IN-SA-PR.AT-2-01	L'Amministrazione implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
IN-SA-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
IN-SA-PR.DS-5-01	L'Amministrazione implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))
IN-SA-PR.DS-6-01	L'Amministrazione implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
IN-SA-PR.IP-1-01	L'Amministrazione implementa la sotto-categoria PR.IP-1 del FNCS. (Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. Principio di minima funzionalità))
IN-SA-PR.IP-12-01	L'Amministrazione implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
IN-SA-PR.IP-4-01	L'Amministrazione implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
IN-SA-PR.IP-9-01	L'Amministrazione implementa la sotto-categoria PR.IP-9 del FNCS. E' stato predisposto il piano di Disaster recovery. Sono state adottate formali procedure di emergenza in caso di indisponibilità parziale dei servizi. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
IN-SA-PR.MA-1-01	L'Amministrazione implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)

IN-SA-PR.MA-2-01	L'Amministrazione implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati)
IN-SA-RC.RP-1-01	L'Amministrazione implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
IN-SA-RS.MI-3-01	L'Amministrazione implementa la sotto-categoria RS.MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)
SC-IP-01	L'ambiente cloud del servizio deve essere accessibile tramite delle API per la gestione remota. Le API esposte devono consentire l'implementazione di automatismi per la gestione remota del ciclo di vita del servizio cloud qualificato. In aggiunta, deve essere prevista la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-02	Per tutte le API esposte dal servizio cloud deve essere dichiarata l'eventuale conformità al Modello di interoperabilità emanato da AgID. Il Modello è descritto dalle linee guida riportate nella circolare AgID, n. 1 del 9 settembre 2020 e i relativi allegati, e dalle ssm. Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).
SC-IP-03	I servizi SaaS devono esporre opportune API di tipo SOAP e/o REST associate alle funzionalità applicative. Tali API devono prevedere la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-04	Il servizio cloud deve garantire la disponibilità di funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati garantendo l'utilizzo di formati open non proprietari.
SC-PS-01	Il servizio cloud deve garantire le seguenti caratteristiche come da indicazioni NIST SP 800-145 e ISO/IEC 17788:2014: 1) Self-Service provisioning: all'utente deve essere garantito di poter provvedere alla fornitura delle risorse informatiche secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Le richieste di risorse computazionali inerenti al servizio cloud oggetto di qualificazione (o informatiche) devono essere fornite unilateralmente, senza la verifica o l'approvazione del fornitore. 2) Accesso alla rete: per il servizio cloud oggetto di qualificazione devono essere offerte opzioni multiple di connettività alla rete e una di queste deve essere obbligatoriamente basata su rete pubblica (i.e. Internet). 3) Pool di risorse: le risorse informatiche relative al servizio oggetto di qualificazione devono essere offerte in un pool, in modo da servire più utenti tramite un modello multi- tenant con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda degli utenti. 4) Elasticità rapida: deve essere supportato il provisioning e de-provisioniag del servizio cloud oggetto di qualificazione. 5) Servizio misurabile: la fornitura a consumo del servizio cloud oggetto di qualificazione deve essere tale che l'utilizzo possa essere monitorato, controllato, segnalato e fatturato; 6) Multi-tenant: le risorse fisiche o virtuali relative al servizio oggetto di qualificazione devono essere allocate in modo tale che più tenant e relative computations e dati siano isolati e inaccessibili l'uno dall'altro.
SC-PS-02	In merito alla scalabilità del servizio cloud, devono essere gestiti e dichiarati i seguenti aspetti: - il meccanismo di scalabilità offerto (automatico e configurabile, nativo, manuale); - la tipologia (orizzontale e/o verticale); - condizione massime di carico sopportabili dal servizio (numero di utenti concorrenti e/o volume di richieste processabili); - le modalità di configurazione (sulla base di metriche di monitoraggio, pianificato nel tempo); - i tempi minimi di reazione del servizio alla richiesta di nuove risorse (i.e. attivazione di nuove risorse). In aggiunta, il fornitore rende disponibili informazioni trasparenti in merito ad eventuali ulteriori funzionalità accessorie disponibili per il servizio e configurabili dall'Amministrazione acquirente per gestire la scalabilità ed ottenere parametri migliori.
SC-QU-01	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione della qualità in conformità allo standard ISO/IEC 9001.
SC-QU-02	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione dei servizi IT in conformità allo standard ISO/IEC 20000.

SC-QU-03	Per il servizio cloud devono essere garantite attività di supporto ai clienti. Il servizio di supporto deve essere: (I) fornito esclusivamente in lingua italiana durante le business hours, anche in lingua inglese per le emergenze 24/7; (II) accessibile almeno tramite uno dei seguenti canali preferenziali: recapito telefonico ed e-mail. In aggiunta, deve essere messo a disposizione dell'Amministrazione Acquirente un sistema di troubleshooting, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i casi di supporto.
SC-SI-DE.CM-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
SC-SI-DE.CM-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
SC-SI-DE.CM-7-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
SC-SI-DE.CM-8-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)
SC-SI-ID.AM-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-1 del FNCS. (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
SC-SI-ID.AM-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-2 del FNCS. (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
SC-SI-ID.AM-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-3 del FNCS. (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
SC-SI-ID.AM-6-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-6 del FNCS. (Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner))
SC-SI-ID.RA-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)
SC-SI-ID.RA-5-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
SC-SI-PR.AC-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
SC-SI-PR.AC-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
SC-SI-PR.AC-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
SC-SI-PR.AC-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
SC-SI-PR.AT-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
SC-SI-PR.AT-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
SC-SI-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
SC-SI-PR.DS-5-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))

SC-SI-PR.DS-6-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
SC-SI-PR.IP-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-1 del FNCS. (Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. Principio di minima funzionalità))
SC-SI-PR.IP-12-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
SC-SI-PR.IP-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
SC-SI-PR.IP-9-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-9 del FNCS. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
SC-SI-PR.MA-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)
SC-SI-PR.MA-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati))
SC-SI-RC.RP-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
SC-SI-RS.MI-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RS MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)

16.2.3 Requisiti ACN-Allegato A2

Requisiti Dati Ordinari

ID Requisito	Specifica Requisito
A.AA-1	1.L'indice di disponibilità dell'Infrastruttura Digitale deve essere stato almeno pari al valore di riferimento corrispondente per il servizio (SL1) così come indicato in Tabella 1 "Indicatori minimi di Servizio dell'Infrastruttura".
A.AA-2	1.Il Centro di elaborazione dati (CED) deve essere dotato di soluzioni hardware e software (apparati di rete e sicurezza, storage, servizi di virtualizzazione, etc.) per la configurazione dei servizi in alta affidabilità. Devono essere inoltre messe a disposizione capability e funzionalità a supporto di configurazioni dei servizi in alta affidabilità quali. a. Scelta della replica locale dei dati per un servizio storage; b. Presenza di servizi di bilanciamento di carico; c. Meccanismi di anti-affinity per la distribuzione delle istanze computazionali

ID Requisito	Specifica Requisito
ID.AM-1	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto 2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati
ID.AM-3	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi all'infrastruttura digitale, sono identificati ed approvati da attori interni al soggetto
ID.AM-6	1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità per tutto il personale e per eventuali terze parti. 2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato 3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sull'infrastruttura. 4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.
PR.AT-1	1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti 2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto in relazione ai ruoli, prevede, almeno, le seguenti tematiche: a. la tutela della confidenzialità di dati in chiaro o cifrati; b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro; d. la definizione di ruoli e delle responsabilità e politiche di accesso a sistemi, asset e risorse; f. politiche di gestione delle informazioni e della sicurezza g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi h. requisiti per la non divulgazione/confidenzialità di informazioni
PR.AT-2	1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti 2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.

ID Requisito	Specifica Requisito
PR.DS-1	1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza 2. Con riferimento alle infrastrutture, al trattamento dei dati e dei servizi dell'Amministrazione, resta fermo quanto previsto dall'allegato A al Regolamento, requisito IN-SA-PR-DS-1-01. 3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto: a. segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE; b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione.
PR.DS-5	1. Sono definite in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per l'accesso ai dati, b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.
PR.DS-6	1. Sono definite in relazione alla categoria ID.AM, almeno: a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni; b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
ID.GV-1	1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.
A.GP-1	1.Sono adottati processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2.
A.GP-2	1. Il soggetto deve garantire per i servizi del Centro di elaborazione dati (CED) offerti attività di supporto in conformità con gli obiettivi (SLO) identificati per i corrispondenti indicatori di servizio (SLI) riportati nella Tabella 1. 2. Il servizio di supporto deve essere: a. fornito esclusivamente in lingua italiana durante le business hours b. accessibile preferenzialmente tramite i seguenti canali: recapito telefonico ed e-mail.

ID Requisito	Specifica Requisito
PR.AC-1	1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza. 2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili per la consultazione, all'Amministrazione. 3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso. 4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale). 5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza. 6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.
PR.AC-2	1. Con riferimento ai censimenti della sottocategoria ID.AM-1, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici; b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi
PR.AC-3	1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity 2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzati degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio. 3. È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione. 4. Esiste un log degli accessi eseguiti da remoto.
PR.AC-4	1. Sono definite con riferimento ai censimenti di cui alla categoria ID.AM, almeno: a. le risorse censite a cui è necessario accedere, per quali funzioni e con quali autorizzazioni; b. I gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni; c. l'assegnazione degli utenti censiti a gruppi di utenti 2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo 3. Sono definite e implementate politiche e procedure, misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate

ID Requisito	Specifica Requisito
PR.IP-1	1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale
PR.IP-12	1. Esiste un documento aggiornato di dettaglio che indica almeno: a. le politiche di sicurezza adottate per gestire le vulnerabilità b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza 2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale
PR.IP-4	1. Viene effettuato periodicamente un backup dei dati memorizzati. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup 2. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"
PR.MA-2	1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti 2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali
RS.MI-3	1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione 2. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.
CE.CE-01	1. La capacità elaborativa dell'Infrastruttura Digitale è gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.
RE.GE-01	1. Il soggetto ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064) o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)
RE.GE-02	1. Il soggetto determina con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti 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 per gli apparati.

ID Requisito	Specifica Requisito
S.DC-01	1. Il soggetto garantisce il presidio operativo del Data Center 24/7/365 2. Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi 3. Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea. 4. Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti 5. Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
S.DC-02	1. Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste policy e procedure dovranno essere riviste su base almeno annuale. 2. Sono implementati, mantenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato 3. Sono implementati, mantenuti e adottati, all'interno dei Data Center, i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.
A.PS-1	1. Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite: bandwidth di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.
RC.RP-1	1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.
ID.RA-1	1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dell'infrastruttura digitale e dell'efficacia delle misure di sicurezza tecniche e procedurali che contiene, inoltre, la periodicità e la modalità di esecuzione. 2. Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).
ID.RA-5	1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate 2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale. 3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
DE.CM-1	1. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS) 2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.

ID Requisito	Specifica Requisito
DE.CM-4	1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonchè sistemi di protezione delle postazioni terminali (Endpoint Protection Systems) 2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.
DE.CM-8	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment, prima della loro messa in esercizio 2. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software 3. Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti 4. Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.
RS.AN-5	1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto 2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonchè di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati. 3. Esiste un documento aggiornato che descrive almeno: a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2; b. i processi, i ruoli e le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2

ID Requisito	Specifica Requisito
DE.AE-3	1. Ai fini di rilevare tempestivamente incidenti con impatto sul servizio cloud, sono adottati gli strumenti tecnici e procedurali per: a. acquisire le informazioni da più sensori e sorgenti; b. ricevere e raccogliere informazioni inerenti alla sicurezza del servizio cloud rese note dal CSIRT Italia, da fonti interne o esterne al soggetto; c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a) e b), per rilevare tempestivamente eventi di interesse. 2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi. 3. Sono definite: a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a); b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b); c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c); d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2. 4. Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale. 5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati 6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile. 7. Nell'ambito delle attività di logging e monitoraggio, in relazione al servizio cloud sono forniti strumenti di gestione degli errori e logging che consentono all'Amministrazione di definire il periodo di custodia (retention) desiderato e di ottenere informazioni sullo stato di sicurezza del servizio cloud, nonché sui dati e le funzioni che fornisce. Le informazioni devono essere sufficientemente dettagliate da consentire la verifica dei seguenti aspetti, nella misura in cui sono applicabili al servizio cloud: a. Quali dati, servizi o funzioni disponibili per l'utente all'interno del servizio cloud sono stati consultati da chi e quando (Audit Logs); b. Malfunzionamenti durante l'elaborazione di azioni automatiche o manuali. 8. Per il servizio oggetto di qualificazione deve essere garantita la possibilità di integrare i log nel sistema SIEM di gestione e monitoraggio dell'Amministrazione e che i Medi log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.
ID.AM-1	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto 2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quell
ID.AM-2	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto. 2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate 3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento nonchè la gestione non autorizzata degli asset dell'organizzazione.
ID.AM-3	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati ed approvati da attori interni al soggetto

ID Requisito	Specifica Requisito
ID.AM-6	1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti. 2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato. 3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sul servizio cloud. 4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.
PR.AT-1	1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti. 2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche: a. la tutela della confidenzialità di dati in chiaro o cifrati. b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro d. la definizione di ruoli e delle responsabilità e. politiche di accesso a sistemi, asset e risorse f. politiche di gestione delle informazioni e della sicurezza g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi h. requisiti per la non divulgazione/confidenzialità di informazioni
PR.AT-2	1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti. 2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.
PS.CA-1	1. Il servizio cloud garantisce almeno le seguenti caratteristiche, come da indicazioni NIST SP 800-145: a. self.service provisioning: il servizio cloud provvede unilateralmente alla fornitura delle risorse informatiche (ad esempio, server e storage in cloud), secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Il servizio cloud soddisfa unilateralmente le richieste dell'Amministrazione di risorse computazionali (o informatiche), senza esplicita verifica o approvazione. b. accesso alla rete: il servizio cloud offre opzioni multiple di connettività alla rete, di cui almeno una basata su rete pubblica (es., Internet). c. elasticità: il soggetto implementa meccanismi automatici di provisioning e deprovisioning del servizio, salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.

ID Requisito	Specifica Requisito
RS.CO-1	1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto. 2. Sono eseguite periodicamente esercitazioni. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2; b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2; c. le modalità per le esercitazioni di cui al punto 3.
RS.CO-5	1. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e altre entità rilevanti e in linea con il contesto del soggetto. 2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.
PR.DS-1	1.Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud al trattamento dei dati e dei servizi dell'Amministrazione, fermo restando quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PRDS-1-01, qualora sussistano motivate e documentate limitazioni di carattere tecnico, eventuali metadati necessari per l'erogazione del servizio cloud possono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate al di fuori del territorio dell'Unione europea. In tal caso, i citati metadati non possono contenere, anche in parte, i dati dell'Amministrazione. 3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto: a. segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE; b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione. 4. Il soggetto garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche e, in particolare: a. Esiste un documento aggiornato di dettaglio inerente alle procedure di crittografia, alla cifratura e alla gestione delle chiavi, le quali dovranno essere aggiornate almeno su base annuale, e recante un'indicazione puntuale di ruoli e responsabilità; b. È prevista una verifica periodica di sistemi, politiche e processi di crittografia e gestione delle chiavi in risposta all'aumento dell'esposizione al rischio, valutato mediante audit da eseguire con cadenza almeno annuale o dopo qualsiasi evento di sicurezza. c. È prevista la generazione di chiavi crittografiche mediante l'utilizzo di librerie crittografiche, con un'indicazione in merito all'algoritmo e al generatore di numeri casuali utilizzati. d. È prevista la generazione di chiavi crittografiche segrete e private per uno scopo unico. e. Sono previsti meccanismi di rotazione delle chiavi crittografiche secondo il periodo di validità delle stesse, tenendo conto di possibili rischi e requisiti normativi e legali. 5. Sono presenti processi, procedure e misure tecniche per revocare e rimuovere le chiavi crittografiche prima della fine del loro periodo di validità, quando una chiave è compromessa, o un'entità non fa più parte dell'organizzazione, conformemente a requisiti legali e normativi. 6. Sono definiti e implementati processi, procedure e misure per la creazione, disattivazione di chiavi al momento della scadenza, eventuali sospensioni e meccanismi di gestione per le chiavi d'accesso a repository
PR.DS-2	1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.

ID Requisito	Specifica Requisito
PR.DS-3	1. Sono definite in relazione alla categoria ID.AM: a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.DS-5	1. Sono definite in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per l'accesso ai dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.
PR.DS-6	1. Sono definiti in relazione alla categoria ID.AM, almeno: a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni; b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.DS-7	1. Sono definite in relazione alla categoria ID.AM: a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata; b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.DP-1	1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese noteall'interno del soggetto. 2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. i ruoli, i processi e le responsabilità di cui al punto 2; b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2. 4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate (PaaS, SaaS).

ID Requisito	Specifica Requisito
IP.GR-1	1. L'ambiente del servizio cloud deve essere accessibile tramite delle interfacce API per la gestione remota dei servizi, assicurando che le API esposte consentano l'implementazione di strumenti per la gestione automatica e remota del ciclo di vita del servizio cloud. 2. È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.
ID.GV-1	1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity. 2. Il Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.
ID.GV-4	1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity. 2. Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy del cloud.
PR.AC-1	1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza. 2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione. 3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso. 4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale). 5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza. 6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.
PR.AC-3	1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity. 2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio. 3. È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione. 4. Esiste un log degli accessi eseguiti da remoto.

ID Requisito	Specifica Requisito
PR.AC-4	1. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno: a. le risorse censite a cui è necessario accedere, con riferimento alla categoria ID.AM, per quali funzioni e con quali autorizzazioni; b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni; c. l'assegnazione degli utenti censiti a gruppi di utenti. 2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo. 3. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.
PR.AC-5	1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale. 2. È presente una pianificazione per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste
PR.AC-7	1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati. 2. In relazione al servizio cloud, deve essere garantita all'Amministrazione la funzionalità di autenticazione a più fattori o l'uso di soluzioni di autenticazione a più fattori di terze parti. Devono essere rese disponibili informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori accessibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).
PR.IP-1	1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale. [IaaS, SaaS]
PR.IP-12	1. Esiste un documento aggiornato di dettaglio che indica almeno: a. le politiche di sicurezza adottate per gestire le vulnerabilità; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale. [SaaS]

ID Requisito	Specifica Requisito
PR.IP-3	1. Sono definite: a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione. 3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.
PR.IP-4	1. Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Viene effettuato periodicamente un backup dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup 3. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette con crittografia forte ed archiviate regolarmente in siti remoti (nel rispetto di quanto previsto dalla categoria PR.DS). Qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta con crittografia forte. 4. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella "Indicatori minimi della qualità del Servizio"
PR.IP-9	1. L'impatto derivante da interruzioni di business ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity. 2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia. 3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte. 4. I piani di business continuity sono collaudati e comunicati alle parti interessate. 5. La documentazione di cui al punto 2 è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.
IP.IN-1	Il servizio SaaS espone opportune API di tipo SOAP e/o REST verso l'Amministrazione associate alle funzionalità applicative, prevedendo in particolare la tracciabilità delle versioni disponibili e la tracciabilità delle richieste ricevute ed evase. Inoltre, è disponibile documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint [SaaS]

ID Requisito	Specifica Requisito
QU.LS-1	1. Il soggetto garantisce aderenza agli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) riportati in Tabella 1 Indicatori della Qualità del Servizio- e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SIA). Il soggetto può comunicare all'Amministrazione eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali. 2. Il soggetto garantisce che venga definita la modalità di condivisione delle informazioni dei livelli di servizio atteso garantiti (SIA) del servizio cloud con l'Amministrazione (es. report periodico) e che, qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Amministrazione per ottenerne la sua approvazione. 3. Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'Amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura del servizio qualificato. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.
QU.LS-2	1. All'interno dei Service Level Agreement (SIA) tra il soggetto e l'Amministrazione sono presenti limitazioni con riferimento a modifiche che abbiano impatto direttamente sugli ambienti e/o tenant di proprietà dell'Amministrazione.
QU.LS-3	1. Ogni SLA tra il soggetto e l'Amministrazione tiene conto di quanto segue: a. Ambito, caratteristiche e ubicazione della relazione commerciale e dei servizi offerti; b. Requisiti di sicurezza delle informazioni (incluso il SSRM - Shared Security Responsibility Mode); c. Processo di Change Management; d. Logging e Monitoring; e. Gestione degli incidenti e procedure di comunicazione; f. Diritto di audit e valutazione da parte di terzi; g. Terminazione del servizio; h. Requisiti di interoperabilità e portabilità; i. Riservatezza dei dati.
QU.LS-4	1. Il soggetto rende disponibile all'Amministrazione l'accesso ad uno o più strumenti di monitoraggio per il servizio cloud. Essi devono consentire attività di raccolta, monitoraggio, filtraggio, creazione di report attraverso parametri predefiniti o parametrizzabili e consentire all'Amministrazione di impostare allarmi personalizzati. La granularità massima delle operazioni non deve essere superiore al minuto (ad es., deve essere possibile filtrare o raccogliere gli eventi ogni minuto). In aggiunta, il soggetto specifica l'eventuale disponibilità di API e strumenti di monitoraggio di terze parti integrate nativamente con il servizio qualificato.
PR.MA-1	1. Sono definite anche in relazione alla categoria ID AM, almeno: a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

ID Requisito	Specifica Requisito
PR.MA-2	1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti. 2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali. 3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi. 4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili. 5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
IP.PO-1	1. Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.
IP.PO-2	1. Sono definite politiche e procedure per l'interoperabilità e la portabilità, le quali vengono riviste e aggiornate almeno su base annuale, compresi requisiti per: a. Comunicazioni tra le interfacce delle applicazioni; b. Interoperabilità del trattamento delle informazioni; c. Portabilità dello sviluppo di applicazioni; d. Scambio, uso, portabilità, integrità e persistenza delle informazioni/dati. [PaaS, SaaS] 2. Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS] 3. Sono incluse, all'interno degli accordi disposizioni che specifichino l'accesso dell'Amministrazione ai dati al termine del contratto, inclusi: a. Formato dei dati; b. Durata del tempo in cui i dati saranno conservati; c. Portata dei dati conservati e messi a disposizione dell'Amministrazione; d. Politica di cancellazione dei dati. [PaaS, SaaS]
QU.PR-1	1. Il soggetto rende disponibile all'Amministrazione strumenti (es una dashboard) ed API che permettono di acquisire informazioni di dettaglio sulle metriche per il calcolo dei costi del servizio doud (cd. di "billing") per rendere il calcolo trasparente all'Amministrazione. Le metriche per il calcolo dei costi del servizio cloud devono essere espresse a livello sintetico o dettagliate per indirizzo di costo (es. risorsa doud). 2. Gli strumenti e le API di cui al punto 1 permettono di filtrare e creare report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account o prodotto in uso del servizio cloud. Il tracciamento e l'aggiornamento delle informazioni sul costo deve essere aggiornato almeno una volta ogni ora.
QU.PR-2	1. Il soggetto offre all'Amministrazione un sistema di monitoraggio dei costi che permetta di impostare allarmi con notifiche per avvisare l'Amministrazione nel caso in cui l'utilizzo del servizio doud si avvicina o supera il budget/le soglie impostate.

ID Requisito	Specifica Requisito
QU.PR-3	1. Il soggetto specifica all'Amministrazione il proprio metodo e modello di determinazione dei prezzi per la fornitura del servizio cloud, che deve assicurare la massima flessibilità commerciale e supportare scalabilità e crescita. 2. Il soggetto fornisce all'Amministrazione: a. un documento contenente i termini e le condizioni, specificando in particolare qualora i prezzi siano forniti per un servizio al consumo e se sono in atto politiche di adeguamento dinamico dei prezzi al mercato; b. un documento contenente i prezzi (i riferimenti ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento completo di listino/prezzi).
PR.PT-1	1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi. 2. Sono definite: a. le politiche di sicurezza adottate per la gestione dei log dei sistemi b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.
PR.PT-5	1. In relazione ai piani previsti dalla sottocategoria a. sono adottate architetture ridondate di rete, di connettività, nonché applicative; 2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate. 3. Sono definite: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
QU.SE-1	1.Il sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN ISO 9001:2015-Sistemi di Gestione per la Qualità. 2. Il sistema di gestione dei servizi IT del servizio cloud è adottato formalmente dal soggetto in conformità allo standard ISO/IEC 20000-1:2018-Sistema di gestione dei servizi IT.
QU.SE-2	1. È garantito il servizio di supporto e assistenza all'Amministrazione per il servizio cloud. 2. Il servizio di supporto e assistenza di cui al punto 1 è fornito almeno in lingua italiana tutti i giorni dell'anno a qualsiasi orario (24/7/365). 3. Il servizio di supporto e assistenza di cui al punto 1 è accessibile almeno tramite recapito telefonico e posta elettronica. 4. Il servizio di supporto e assistenza di cui al punto 1 prevede, inoltre, un sistema di risoluzione dei problemi (troubleshooting) a disposizione dell'Amministrazione, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).
QU.SE-3	1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).

ID Requisito	Specifica Requisito
QU.SE-4	1. Devono essere rese disponibili all'Amministrazione le linee guida per una gestione sicura del servizio cloud oggetto di qualificazione, indirizzando, ove applicabile, i seguenti aspetti: a. Istruzioni per una configurazione sicura; b. Informazione su vulnerabilità note e meccanismi di aggiornamento; c. Gestione degli errori e meccanismi di logging; d. Meccanismi di autenticazione; e. Ruoli e diritti, comprese le combinazioni che risultano in un rischio elevato; f. Servizi e funzioni per l'amministrazione del servizio da parte di utenti privilegiati; g. Le linee guida vengono fornite e mantenute nelle modalità e tempistiche di cui alla misura 1P.GR-01.
RC.RP-1	1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.
RS.RP-1	1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sul servizio cloud.
ID.RA-1	1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica del servizio cloud e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione. 2. Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).
ID.RA-5	1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate. 2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud. 3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
PS.SC-1	1. Il soggetto comunica all'Amministrazione: a. il meccanismo di scalabilità offerto (es. automatico e configurabile, nativo, manuale); b. la tipologia (orizzontale e/o verticale); c. le condizioni massime di carico sopportabili dal servizio (es. numero di utenti concorrenti e/o volume di richieste processabili); d. le modalità di configurazione (es. sulla base di metriche di monitoraggio, pianificato nel tempo); e. i tempi minimi di reazione del servizio alla richiesta di nuove risorse (es. attivazione di nuove risorse).

ID Requisito	Specifica Requisito
DE.CM-1	1. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS). 2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante. 3. È previsto un sistema di monitoraggio dei degli accessi al fine di rilevare attività sospette e stabilire un processo definito per l'adozione di azioni appropriate e tempestive in risposta alle anomalie rilevate
DE.CM-4	1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection Systems - EPS). 2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.
ID.SC-1	1. Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber. 2. Tali processi sono validati e approvati da parte dei vertici del soggetto

Requisiti Dati Critici

ID Requisito	Specifica Requisito
RS-AN-5	1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e del penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-8 qualora disponibili, sono diffusi alle articolazioni competenti del soggetto 2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019 dell'Autorità di riferimento del proprio settore produttivo, nonchè di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati. 3. Esiste un documento aggiornato che descrive, almeno: a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2; b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2

ID Requisito	Specifica Requisito
DE.AE-3	1. Ai fini di rilevare tempestivamente incidenti con impatto dell'infrastruttura, sono adottati gli strumenti tecnici e procedurali per: a. acquisire le informazioni da più sensori e sorgenti; b. ricevere e raccogliere informazioni inerenti alla sicurezza dell'infrastruttura rese note dal CSIRT Italia, da fonti interne o esterne al soggetto; c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a), b) e c), per rilevare tempestivamente eventi di interesse 2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi. 3. Sono definite: a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a); b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b); c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c). d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2. 4 Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale 5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati. 6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile
ID.AM-2	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto. 2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate 3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonchè gestione non autorizzata degli asset dell'organizzazione
ID.AM-6	1. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto. 2. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto. 3. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale, anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021, e alle attività di verifica e ispezione
A.BC-3	1. Provider di infrastruttura: L'infrastruttura digitale è dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 12 ore e RPO 12 ore. 2. Public Cloud provider: devono essere presenti servizi cloud di Disaster Recovery

ID Requisito	Specifica Requisito
RS.CO-1	1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto. 2. Sono eseguite periodicamente esercitazioni. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2; b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2; c. le modalità per le esercitazioni di cui al punto 3
RS.CO-5	1. Sono definiti e mantenuti contatti con gruppi di interesse legati all'infrastruttura digitale e altre entità rilevanti e in linea con il contesto del soggetto in relazione all'infrastruttura digitale. 2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.
PR.DS-2	1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati
PR.DS-3	1. Sono definite in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.DS-7	1. Sono definite in relazione alla categoria ID.AM, almeno: a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
DE.DP-1	1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese note all'interno del soggetto. 2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. i ruoli, i processi e le responsabilità di cui al punto 2; b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2. 4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che convolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate.
ID.GV-1	2. Il documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione

ID Requisito	Specifica Requisito
ID.GV-4	1. Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy dell'infrastruttura.
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6, b. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.AC-2	3. È definito un perimetro di sicurezza tra le aree amministrative e le aree di data storage e processing
PR.AC-3	5. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate; b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.AC-4	4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1
PR.AC-5	1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale 2. È definito un piano per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste
PR.AC-7	1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati
PR.IP-3	1. Sono definite: a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza 2. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione. 3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza
PR.IP-4	3. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

ID Requisito	Specifica Requisito
PR.IP-9	1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dall'Infrastruttura digitale 2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani c. i ruoli e le responsabilità del personale d. i flussi di comunicazione e reportistica e. il raccordo con il CSIRT Italia 3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte 4. I piani di business continuity sono collaudati e comunicati alle parti interessate 5. La documentazione di cui al punto 2 è resa disponibile all'Amministrazione e rivista periodicamente 6. L'impatto derivante da interruzioni ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.
PR.MA-1	1 Sono definite in relazione alla categoria ID.AM: a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi; b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.MA-2	3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi 4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili 5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
A.DC-1	1. L'infrastruttura digitale deve aderire ai parametri del certificato ANSI/TIA 942B con rating "Concurrent Maintainability" oppure a quello di Tier III dell'Uptime Institute In alternativa deve essere conforme alle caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio riportati alla Tabella 2.
PR.PT-1	1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi. 2. Sono definite: a. le politiche di sicurezza adottate per la gestione dei log dei sistemi b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log

ID Requisito	Specifica Requisito
PR.PT-5	1. In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architetture ridondate di rete, di connettività, nonchè applicative; 2. Esistono meccanismi per garantire la continuità operativa nel rispetto delle misure di sicurezza qui elencate. 3. Sono definite: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
RC.RP-1	2. Il piano di ripristino viene testato su base semestrale nell'ambito di due esercitazini annuali
RS.RP-1	1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE, nonchè la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto anche ai fini della notifica all'Amministrazione e, su base volontaria al CSIRT Italia, degli incidenti con impatto sull'infrastruttura digitale.
ID.RA-5	4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno: a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento b. le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DE.CM-8; c. i potenziali impatti ritenuti significativi sull'infrastruttura digitale, opportunamente descritti e valuatati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-7	1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi si sorveglianza e controllo di accesso, anche automatizzati 2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete. 3. Gli strumenti tecnici di cui ai punti 1 e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC, e PR.DS. 4. Esiste un documento aggiornato che descrive almeno: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
ID.SC-1	1. Esiste un documento aggiornato di dettaglio che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber. 2. Tali processi sono validati e approvati da parte dei vertici del soggetto
DE.AE-3	9. Esiste un repository centralizzato che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto

ID Requisito	Specifica Requisito
ID.AM-6	5. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN). 6. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto. 7. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto. 8. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021.
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
RC.CO-3	1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. Le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT)
RS.CO-1	4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned). 5. Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discoveiy e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale. 6. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza. 7. È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili. 8. Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione In particolare, le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale interlocuzione con il CSIRT Italia.

ID Requisito	Specifica Requisito
PR.DS-1	7. Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui alla sezione 2.2.7, PR.DS-1, punto 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud, nonché al trattamento dei dati e dei servizi dell'Amministrazione, ivi inclusi i metadati, resta fermo, pertanto, quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01. 8. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria IDAM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza 9. Il servizio cloud supporta un meccanismo di cifratura di tipo Bring Your Own Key (BYOK), che consente all'Amministrazione di generare autonomamente, almeno la chiave principale di cifratura (root key), attraverso un HSM ospitato, alternativamente, presso: a. propria infrastruttura b. infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata c. infrastruttura di una terza parte scelta dall'Amministrazione. 10. Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 10 nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud. 11. Sono definite ed implementate procedure e misure tecniche misure per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi. 12. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.
PR.DS-3	2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti [SaaS] 3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto [SaaS]
ID.GV-1	3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato 4. Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6, b. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza

ID Requisito	Specifica Requisito
PR.AC-3	5. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate; b. I processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
PR.AC-4	4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1
PR.IP-1	2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e il dispiegamento delle sole configurazioni adottate; b l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. [SaaS] 3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni 4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità 5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile. 6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS] 7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].
PR.IP-12	3. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management 4. Il documento di cui al punto 1 della misura PR.IP-12 dovrà essere aggiornato su base semestrale.
PR.IP-2	1. Sono implementate linee guida e misure tecniche/organizzative per lo sviluppo sicuro del servizio cloud, in aderenza alle linee guida OWASP in merito alla sicurezza nello sviluppo del software (requisiti, progettazione, implementazione, test e verifica). Devono essere resi disponibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e alla Amministrazione i report sui test OWASP condotti, garantendo l'assenza di vulnerabilità di tipo "high" o "critical".
PR.IP-4	5. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 6. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

ID Requisito	Specifica Requisito
PR.IP-9	6. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal servizio cloud e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery, 7. Esiste un documento aggiornato di dettaglio contenente i piani di disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia 8. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte. 9. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate. 10. I dispositivi critici per il funzionamento del servizio cloud sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore
PR.MA-1	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1. 3. Le attività di cui al punto 3 sono volte a verificare anche aspetti di sicurezza. 4. Gli aggiornamenti software sono consentiti solo da fonti pre-autorizzate. 5. Tutti i log relativi alle attività di manutenzione e aggiornamento sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività 6. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 3, 4, e 5
RS.MI-3	1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione. 2. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.
PR.PT-5	1-bis. In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architettura ridondate di rete, di connettività, nonché applicative. b. esiste un sito di disaster recovery.
RC.RP-1	3. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

ID Requisito	Specifica Requisito
RS.RP-1	2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale. 3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate. 4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi 5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity. 6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza. 7. Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.
ID.RA-1	3. Le relazioni periodiche delle verifiche e dei test di cui al punto 1 devono contenere almeno: a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse; b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza; c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità. 4. Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.
ID.RA-5	4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno: a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento; b. le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DECM-8; c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-1	5. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity. 6. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono aggiornati, manutenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono impiegati anche per i fini di cui alla categoria DE.AE 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 3, 4 e 5; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

ID Requisito	Specifica Requisito
DE.CM-4	4. Sono configurati appositi software firewall su tutti i dispositivi. 5. I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox. 6. Gli strumenti tecnici di cui ai punti 1, 4 e 5 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 7. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-7	1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati. 2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete. 3. Gli strumenti tecnici di cui ai punti le 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 4. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-8	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration teste vulnerability assessment, prima della loro messa in esercizio. 2. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software. 3. Esiste un documento aggiornato recante la tipologia di penetration teste vulnerability assessment previsti. 4. Esiste un registro aggiornato dei penetration teste vulnerability assessment eseguiti corredato dalla relativa documentazione.
ID.SC-1	3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (Shared Security Responsibility Model-SSRM) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale. 4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione. 5. È fornita una chiara definizione in merito alla condivisione delle responsabilità.

ID Requisito	Specifica Requisito
ID.SC-2	1. In merito all'affidamento di forniture per i servizi cloud sono adottate misure in materia di sicurezza della catena di approvvigionamento cyber attraverso: a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione; b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore; c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del servizio cloud; d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno: i. della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza; ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo. 2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1.
ID.SC-3	1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.
ID.SC-4	1. Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata. 2. Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione. 3. È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio 4. Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente. 5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation.

Requisiti Dati Strategici

ID Requisito	Specifica Requisito
DE.AE-3	10. Esiste una repository centralizzata che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto. 11. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett. a, b, c, d.
ID.AM-6	8. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
A.BC-4	1. Provider di infrastruttura: L'infrastruttura digitale deve essere dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 8 ore e RPO 8 ore; 2. Public Cloud provider: devono essere presenti servizi di Disaster Recovery
RC.CO-3	1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. Le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).
RS.CO-1	4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned). 5. Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale. 6. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza. 7. È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili. 8. Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione. In particolare, le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale interlocuzione con il CSIRT Italia.
PR.DS-1	4. Sono definite ed implementate procedure e misure tecniche per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi.

ID Requisito	Specifica Requisito
PR.DS-3	2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti. 3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto. 4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1
PR.DS-5	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
ID.GV-1	3. Ogni scostamento dai livello minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato 4. Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti.
PR.AC-3	6. Le politiche e procedure aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, del soggetto. 7. È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati della stessa. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati. Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate
PR.AC-4	5. Il soggetto è autonomo nella gestione dell'infrastruttura, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.
PR.AC-5	3. Con riferimento ai censimenti di cui alla categoria IDAM, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti; b. la descrizione delle reti segregate/segmentate; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza; d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.

ID Requisito	Specifica Requisito
PR.AC-7	2. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla categoria ID.RA, contiene almeno: a. le modalità di autenticazione disponibili; b. la loro assegnazione alle categorie di transazioni.
RC.IM-2	Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.
PR.IP-1	2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e il dispiegamento delle sole configurazioni adottate; b. l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni. 4 Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità 5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni vulnerabilità delle applicazioni, automatizzando la riparazione quando possibile. 6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni. 7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni
PR.IP-11	1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. 2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.
PR.IP-12	2. Il documento di cui al punto 1 della misura PR.IP-12 dovrà essere aggiornato su base semestrale. 3. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

ID Requisito	Specifica Requisito
PR.IP-9	7. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dall'infrastruttura digitale e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery. 8. Esiste un documento aggiornato di dettaglio contenente i piani di disaster recovery nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia 9. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte. 10. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate. 11. I dispositivi critici per il funzionamento dell'infrastruttura sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore.
PR.MA-1	2. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite. 3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1. 4. In base all'analisi del rischio, ogni aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e il relativo codice oggetto dovrà essere custodito per almeno 24 mesi. 5. In base all'analisi del rischio di cui alla misura ID.RA-5, ogni aggiornamento hardware o software di componenti ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e, se del caso, il relativo codice oggetto dovrà essere custodito per almeno 24 mesi. Le attività in ambiente di test sono volte a verificare anche aspetti di sicurezza. 6. Gli aggiornamenti software devono essere consentiti solo da fonti pre-autorizzate. 7. Tutti i log relativi alle attività di manutenzione e aggiornamento dovranno essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività. 8. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 5, 6 e 7.
PR.MA-2	6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.
PR.PT-1	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

ID Requisito	Specifica Requisito
PR.PT-4	1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati. 2. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati. 3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 4. L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA. 5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE. 6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.
PR.PT-5	1-bis. In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architettura ridondate di rete, di connettività, nonché applicative. b. esiste un sito di disaster recovery. 4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3.
RS.RP-1	2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale. 3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate. 4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi. 5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity. 6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza. 7. Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.
ID.RA-1	3. Le relazioni periodiche devono contenere almeno: a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse; b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza; c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità 4. Esiste un documento per la correzione delle vulnerabilità che prevede anche la notifica alle parti interessate

ID Requisito	Specifica Requisito
DE.CM-1	3. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity. 4. Gli strumenti tecnici di cui al punto 1 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PRMA e concorrono al rispetto delle politiche di cui alla categoria IDAM, ID.GV, IDSC, PR.AC e PR.DS. 5. Gli strumenti tecnici di cui al punto 1 sono impiegati anche per i fini di cui alla categoria DE.AE 6. Esiste un documento aggiornato che descrive almeno: a. le politiche di sicurezza adottate in relazione al punto 2; b. i processi, lemetodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-4	4. Sono configurati appositi software firewall su tutti i dispositivi. 5. I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox. 6. Gli strumenti tecnici di cui ai punti 4 e 5 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie I D.AM, ID.GV, I D.SC, PR.AC e PRDS. 7. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3: b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-7	5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento del software non approvati. 6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate. 7. Gli strumenti tecnici di cui ai punti 5 e 6 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PRIP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, I D.SC, PR.AC e PRDS. 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 5 e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
ID.SC-1	3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (Shared Security Responsibility Model - SSRM) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale. 4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi incluse le infrastrutture digitali.

ID Requisito	Specifica Requisito
ID.SC-2	1. In merito all'affidamento di forniture sono adottate misure in materia di sicurezza della catena di approvvigionamento attraverso: a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2. nel processo di fornitura, già a partire dalla fase di progettazione; b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore; c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza dell'infrastruttura digitale; d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno: i. della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo 2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per il funzionamento dell'infrastruttura, nonchè dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1 lettera d. 3. Si raccomanda, ove possibile e in relazione alla criticità di: a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto: i. della disponibilità del fornitore a condividere il codice sorgente; ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore iii. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato all'interno dei beni e dei sistemi di Information and Communication Technology iv. dell'adozione da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato e eseguito. b. adottare processi e strumenti tecnici per: i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore; ii. acquisire il codice oggetto dai beni e i sistemi di Information and Communication Technology iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito.
ID.SC-3	1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate all'infrastruttura digitale. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornate di conseguenza

ID Requisito	Specifica Requisito
ID.SC-4	1. Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata. 2. Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione. 3. È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio 4.Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente. 5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation.
DE.AE-3	9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett a, b, c, d.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
PR.DS-1	13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio di cloud. Il soggetto rende disponibile l'elenco all'Amministrazione
PR.DS-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-5	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.AC-3	6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione. 7. È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati dello stesso. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati. 8. Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate
PR.AC-4	4. Tutte le attività privilegiate (es. installazione di aggiornamenti) e di accesso ai dati dell'Amministrazione da parte del personale del soggetto e di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitate ai soli casi essenziali.

ID Requisito	Specifica Requisito
PR.AC-5	3. Con riferimento ai censimenti di cui alla categoria IDAM, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti; b. la descrizione delle reti segregate/segmentate; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza; d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.
PR.AC-7	3. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla categoria ID.RA, contiene almeno: a. le modalità di autenticazione disponibili; b. la loro assegnazione alle categorie di transazioni
RC.IM-2	1. Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.MA-2	6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.
PR.MA-1	7. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite. 8. In base all'analisi del rischio, ogni aggiornamento del software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo. 9. Il codice oggetto relativo agli aggiornamenti di cui al punto 3 viene custodito per almeno 24 mesi.
PR.PT-1	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett a e b.
PR.PT-4	1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati. 2. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati. 3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 4. L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA. 5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE. 6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.

ID Requisito	Specifica Requisito
PR.PT-5	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.
DE.CM-7	5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati. 6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate. 7. Gli strumenti tecnici di cui ai punti 5 e 6 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 5 e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
ID.SC-1	6. Esiste un documento recante i processi di cui ai punti 1 e 2.
ID.SC-2	3. Si raccomanda, ove possibile e in relazione alla criticità di: a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto: i. della disponibilità del fornitore a condividere il codice sorgente; ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore; iii. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato all'interno dei beni e dei sistemi di information and communication technology; iv. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito. b. adottare processi e strumenti tecnici per: i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore; ii. acquisire il codice oggetto dai beni e sistemi di information and communication technology; iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito
ID.SC-3	2. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.

16.2.4 Requisiti ACN-Allegato B2

Requisiti Dati Ordinari

ID Requisito	Specifica Requisito
RS.AN-5	1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto 2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonchè di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati. 3. Esiste un documento aggiornato che descrive almeno: a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2; b. i processi, i ruoli e le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2
DE.AE-3	1. Al fini di rilevare tempestivamente incidenti con impatto sul servizio cloud, sono adottati gli strumenti tecnici e procedurali per: a. acquisire le informazioni da più sensori e sorgenti; b. ricevere e raccogliere informazioni inerenti alla sicurezza del servizio cloud rese note dal CSIRT Italia, da fonti interne o esterne al soggetto; c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a) e b), per rilevare tempestivamente eventi di interesse. 2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi. 3. Sono definite: a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a); b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b); c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c); d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2. 4. Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale. 5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati 6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile. 7. Nell'ambito delle attività di logging e monitoraggio, in relazione al servizio cloud sono forniti strumenti di gestione degli errori e logging che consentono all'Amministrazione di definire il periodo di custodia (retention) desiderato e di ottenere informazioni sullo stato di sicurezza del servizio cloud, nonché sui dati e le funzioni che fornisce. Le informazioni devono essere sufficientemente dettagliate da consentire la verifica dei seguenti aspetti, nella misura in cui sono applicabili al servizio cloud: a. Quali dati, servizi o funzioni disponibili per l'utente all'interno del servizio cloud sono stati consultati da chi e quando (Audit Logs); b. Malfunzionamenti durante l'elaborazione di azioni automatiche o manuali. 8. Per il servizio oggetto di qualificazione deve essere garantita la possibilità di integrare i log nel sistema SIEM di gestione e monitoraggio dell'Amministrazione e che i Medi log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.

ID Requisito	Specifica Requisito
ID.AM-1	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto 2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli
ID.AM-2	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto. 2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate 3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento nonchè la gestione non autorizzata degli asset dell'organizzazione.
ID.AM-3	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati ed approvati da attori interni al soggetto
ID.AM-6	1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti. 2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato. 3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sul servizio cloud. 4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.
PR.AT-1	1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti. 2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche: a. la tutela della confidenzialità di dati in chiaro o cifrati. b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro d. la definizione di ruoli e delle responsabilità e. politiche di accesso a sistemi, asset e risorse f. politiche di gestione delle informazioni e della sicurezza g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi h. requisiti per la non divulgazione/confidenzialità di informazioni
PR.AT-2	1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti. 2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.

ID Requisito	Specifica Requisito
PS.CA-1	1. Il servizio cloud garantisce almeno le seguenti caratteristiche, come da indicazioni NIST SP 800-145: a. self-service provisioning: il servizio cloud provvede unilateralmente alla fornitura delle risorse informatiche (ad esempio, server e storage in cloud), secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Il servizio cloud soddisfa unilateralmente le richieste dell'Amministrazione di risorse computazionali (o informatiche), senza esplicita verifica o approvazione. b. accesso alla rete: il servizio cloud offre opzioni multiple di connettività alla rete; di cui almeno una basata su rete pubblica (es., Internet). c. elasticità: il soggetto implementa meccanismi automatici di provisioning e deprovisioning del servizio, salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.
RS.CO-1	1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto. 2. Sono eseguite periodicamente esercitazioni. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2; b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2; c. le modalità per le esercitazioni di cui al punto 3.
RS.CO-5	1. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e altre entità rilevanti e in linea con il contesto del soggetto. 2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.

ID Requisito	Specifica Requisito
PR.DS-1	1.Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud al trattamento dei dati e dei servizi dell'Amministrazione, fermo restando quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PRDS-1-01, qualora sussistano motivate e documentate limitazioni di carattere tecnico, eventuali metadati necessari per l'erogazione del servizio cloud possono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate al di fuori del territorio dell'Unione europea. In tal caso, i citati metadati non possono contenere, anche in parte, i dati dell'Amministrazione. 3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto: a. segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE; b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione. 4. Il soggetto garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche e, in particolare: a. Esiste un documento aggiornato di dettaglio inerente alle procedure di crittografia, alla cifratura e alla gestione delle chiavi, le quali dovranno essere aggiornate almeno su base annuale, e recante un'indicazione puntuale di ruoli e responsabilità; b. È prevista una verifica periodica di sistemi, politiche e processi di crittografia e gestione delle chiavi in risposta all'aumento dell'esposizione al rischio, valutato mediante audit da eseguire con cadenza almeno annuale o dopo qualsiasi evento di sicurezza. c. È prevista la generazione di chiavi crittografiche mediante l'utilizzo di librerie crittografiche, con un'indicazione in merito all'algoritmo e al generatore di numeri casuali utilizzati. d. È prevista la generazione di chiavi crittografiche segrete e private per uno scopo unico. e. Sono previsti meccanismi di rotazione delle chiavi crittografiche secondo il periodo di validità delle stesse, tenendo conto di possibili rischi e requisiti normativi e legali. 5. Sono presenti processi, procedure e misure tecniche per revocare e rimuovere le chiavi crittografiche prima della fine del loro periodo di validità, quando una chiave è compromessa, o un'entità non fa più parte dell'organizzazione, conformemente a requisiti legali e normativi. 6. Sono definiti e implementati processi, procedure e misure per la creazione, disattivazione di chiavi al momento della scadenza, eventuali sospensioni e meccanismi di gestione per le chiavi d'accesso a repository
PR.DS-2	1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.
PR.DS-3	1. Sono definite in relazione alla categoria ID.AM: a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
PR.DS-5	1. Sono definite in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per l'accesso ai dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.

ID Requisito	Specifica Requisito
PR.DS-6	1. Sono definiti in relazione alla categoria ID.AM, almeno: a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni; b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
PR.DS-7	1. Sono definite in relazione alla categoria ID.AM: a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata; b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.DP-1	1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese noteall'interno del soggetto. 2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto. 3. Esiste un documento aggiornato di dettaglio che indica almeno: a. i ruoli, i processi e le responsabilità di cui al punto 2; b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2. 4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate (PaaS, SaaS).
IP.GR-1	1. L'ambiente del servizio cloud deve essere accessibile tramite delle interfacce API per la gestione remota dei servizi, assicurando che le API esposte consentano l'implementazione di strumenti per la gestione automatica e remota del ciclo di vita del servizio cloud. 2. È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.
ID.GV-1	1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity. 2. Il Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.
ID.GV-4	1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity. 2. Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy del cloud.

ID Requisito	Specifica Requisito
PR.AC-1	1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza. 2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione. 3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso. 4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale). 5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza. 6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.
PR.AC-3	1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity. 2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio. 3. È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione. 4. Esiste un log degli accessi eseguiti da remoto.
PR.AC-4	1. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno: a. le risorse censite a cui è necessario accedere, con riferimento alla categoria ID.AM, per quali funzioni e con quali autorizzazioni; b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni; c. l'assegnazione degli utenti censiti a gruppi di utenti. 2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo. 3. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.
PR.AC-5	1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale. 2. È presente una pianificazione per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste
PR.AC-7	1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati. 2. In relazione al servizio cloud, deve essere garantita all'Amministrazione la funzionalità di autenticazione a più fattori o l'uso di soluzioni di autenticazione a più fattori di terze parti. Devono essere rese disponibili informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori accessibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).

ID Requisito	Specifica Requisito
PR.IP-1	1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale. [IaaS, SaaS]
PR.IP-12	1. Esiste un documento aggiornato di dettaglio che indica almeno: a. le politiche di sicurezza adottate per gestire le vulnerabilità; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale. [SaaS]
PR.IP-3	1. Sono definite: a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione. 3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.
PR.IP-4	1. Sono definite, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 2. Viene effettuato periodicamente un backup dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati del backup 3. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette con crittografia forte ed archiviate regolarmente in siti remoti (nel rispetto di quanto previsto dalla categoria PR.DS). Qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta con crittografia forte. 4. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella "Indicatori minimi della qualità del Servizio"

ID Requisito	Specifica Requisito
PR.IP-9	1. L'impatto derivante da interruzioni di business ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity. 2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia. 3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte. 4. I piani di business continuity sono collaudati e comunicati alle parti interessate. 5. La documentazione di cui al punto 2 è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.
IP.IN-1	Il servizio SaaS espone opportune API di tipo SOAP e/o REST verso l'Amministrazione associate alle funzionalità applicative, prevedendo in particolare la tracciabilità delle versioni disponibili e la tracciabilità delle richieste ricevute ed evase. Inoltre, è disponibile documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint [SaaS]
QU.LS-1	1. Il soggetto garantisce aderenza agli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) riportati in Tabella 1 Indicatori della Qualità del Servizio· e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA). Il soggetto può comunicare all'Amministrazione eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali. 2. Il soggetto garantisce che venga definita la modalità di condivisione delle informazioni dei livelli di servizio atteso garantiti (SLA) del servizio cloud con l'Amministrazione (es. report periodico) e che, qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Amministrazione per ottenerne la sua approvazione. 3. Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'Amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura del servizio qualificato. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.
QU.LS-2	1. All'interno dei Service Level Agreement (SLA) tra il soggetto e l'Amministrazione sono presenti limitazioni con riferimento a modifiche che abbiano impatto direttamente sugli ambienti e/o tenant di proprietà dell'Amministrazione.

ID Requisito	Specifica Requisito
QU.LS-3	1. Ogni SLA tra il soggetto e l'Amministrazione tiene conto di quanto segue: a. Ambito, caratteristiche e ubicazione della relazione commerciale e dei servizi offerti; b. Requisiti di sicurezza delle informazioni (incluso il SSRM - Shared Security Responsibility Mode); c. Processo di Change Management; d. Logging e Monitoring; e. Gestione degli incidenti e procedure di comunicazione; f. Diritto di audit e valutazione da parte di terzi; g. Terminazione del servizio; h. Requisiti di interoperabilità e portabilità; i. Riservatezza dei dati.
QU.LS-4	1. Il soggetto rende disponibile all'Amministrazione l'accesso ad uno o più strumenti di monitoraggio per il servizio cloud. Essi devono consentire attività di raccolta, monitoraggio, filtraggio, creazione di report attraverso parametri predefiniti o parametrizzabili e consentire all'Amministrazione di impostare allarmi personalizzati. La granularità massima delle operazioni non deve essere superiore al minuto (ad es., deve essere possibile filtrare o raccogliere gli eventi ogni minuto). In aggiunta, il soggetto specifica l'eventuale disponibilità di API e strumenti di monitoraggio di terze parti integrate nativamente con il servizio qualificato.
PR.MA-1	1. Sono definite anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
PR.MA-2	1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti. 2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali. 3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi. 4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili. 5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
IP.PO-1	1. Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.

ID Requisito	Specifica Requisito
IP.PO-2	1. Sono definite politiche e procedure per l'interoperabilità e la portabilità, le quali vengono riviste e aggiornate almeno su base annuale, compresi requisiti per: a. Comunicazioni tra le interfacce delle applicazioni; b. Interoperabilità del trattamento delle informazioni; c. Portabilità dello sviluppo di applicazioni; d. Scambio, uso, portabilità, integrità e persistenza delle informazioni/dati. [PaaS, SaaS] 2. Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS] 3. Sono incluse, all'interno degli accordi disposizioni che specifichino l'accesso dell'Amministrazione ai dati al termine del contratto, inclusi: a. Formato dei dati; b. Durata del tempo in cui i dati saranno conservati; c. Portata dei dati conservati e messi a disposizione dell'Amministrazione; d. Politica di cancellazione dei dati. [PaaS, SaaS]
QU.PR-1	1. Il soggetto rende disponibile all'Amministrazione strumenti (es una dashboard) ed API che permettono di acquisire informazioni di dettaglio sulle metriche per il calcolo dei costi del servizio doud (cd. di -billing") per rendere il calcolo trasparente all'Amministrazione. Le metriche per il calcolo dei costi del servizio cloud devono essere espresse a livello sintetico o dettagliate per indirizzo di costo (es. risorsa doud). 2. Gli strumenti e le API di cui al punto 1 permettono di filtrare e creare report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account o prodotto in uso del servizio cloud. Il tracciamento e l'aggiornamento delle informazioni sul costo deve essere aggiornato almeno una volta ogni ora.
QU.PR-2	1. Il soggetto offre all'Amministrazione un sistema di monitoraggio dei costi che permetta di impostare allarmi con notifiche per avvisare l'Amministrazione nel caso in cui l'utilizzo del servizio doud si avvicina o supera il budget/le soglie impostate.
QU.PR-3	1. Il soggetto specifica all'Amministrazione il proprio metodo e modello di determinazione dei prezzi per la fornitura del servizio cloud, che deve assicurare la massima flessibilità commerciale e supportare scalabilità e crescita. 2. Il soggetto fornisce all'Amministrazione: a. un documento contenente i termini e le condizioni, specificando in particolare qualora i prezzi siano forniti per un servizio al consumo e se sono in atto politiche di adeguamento dinamico dei prezzi al mercato; b. un documento contenente i prezzi (i riferimenti ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento completo di listino/prezzi).
PR.PT-1	1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi. 2. Sono definite: a. le politiche di sicurezza adottate per la gestione dei log dei sistemi b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.

ID Requisito	Specifica Requisito
PR.PT-5	1. In relazione ai piani previsti dalla sottocategoria a. sono adottate architetture ridondate di rete, di connettività, nonché applicative; 2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate. 3. Sono definite: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
QU.SE-1	1.Il sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN ISO 9001:2015-Sistemi di Gestione per la Qualità. 2. Il sistema di gestione dei servizi IT del servizio cloud è adottato formalmente dal soggetto in conformità allo standard ISO/IEC 20000-1:2018-Sistema di gestione dei servizi IT.
QU.SE-2	1. È garantito il servizio di supporto e assistenza all'Amministrazione per il servizio cloud. 2. Il servizio di supporto e assistenza di cui al punto 1 è fornito almeno in lingua italiana tutti i giorni dell'anno a qualsiasi orario (24/7/365). 3. Il servizio di supporto e assistenza di cui al punto 1 è accessibile almeno tramite recapito telefonico e posta elettronica. 4. Il servizio di supporto e assistenza di cui al punto 1 prevede, inoltre, un sistema di risoluzione dei problemi (troubleshooting) a disposizione dell'Amministrazione, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).
QU.SE-3	1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).
QU.SE-4	1. Devono essere rese disponibili all'Amministrazione le linee guida per una gestione sicura del servizio cloud oggetto di qualificazione, indirizzando, ove applicabile, i seguenti aspetti: a. Istruzioni per una configurazione sicura; b. Informazione su vulnerabilità note e meccanismi di aggiornamento; c. Gestione degli errori e meccanismi di logging; d. Meccanismi di autenticazione; e. Ruoli e diritti, comprese le combinazioni che risultano in un rischio elevato; f. Servizi e funzioni per l'amministrazione del servizio da parte di utenti privilegiati; g. Le linee guida vengono fornite e mantenute nelle modalità e tempistiche di cui alla misura 1P.GR-01.
RC.RP-1	1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.
RS.RP-1	1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sul servizio cloud.

ID Requisito	Specifica Requisito
ID.RA-1	1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica del servizio cloud e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione. 2. Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).
ID.RA-5	1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate. 2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud. 3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
PS.SC-1	1. Il soggetto comunica all'Amministrazione: a. il meccanismo di scalabilità offerto (es. automatico e configurabile, nativo, manuale); b. la tipologia (orizzontale e/o verticale); c. le condizioni massime di carico sopportabili dal servizio (es. numero di utenti concorrenti e/o volume di richieste processabili); d. le modalità di configurazione (es. sulla base di metriche di monitoraggio, pianificato nel tempo); e. i tempi minimi di reazione del servizio alla richiesta di nuove risorse (es. attivazione di nuove risorse).
DE.CM-1	1. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS). 2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante. 3. È previsto un sistema di monitoraggio dei degli accessi al fine di rilevare attività sospette e stabilire un processo definito per l'adozione di azioni appropriate e tempestive in risposta alle anomalie rilevate
DE.CM-4	1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection Systems - EPS). 2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.
ID.SC-1	1. Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber. 2. Tali processi sono validati e approvati da parte dei vertici del soggetto

Requisiti Dati Critici

ID Requisito	Specifica Requisito
DE.AE-3	9. Esiste un repository centralizzato che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto
ID.AM-6	5.I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN). 6. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto. 7. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto. 8. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021.
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
RC.CO-3	1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. Le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT)
RS.CO-1	4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned). 5. Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discoveiy e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale. 6. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza. 7. È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili. 8. Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione In particolare, le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale interlocuzione con il CSIRT Italia.

ID Requisito	Specifica Requisito
PR.DS-1	7. Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui alla sezione 2.2.7, PR.DS-1, punto 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud, nonché al trattamento dei dati e dei servizi dell'Amministrazione, ivi inclusi i metadati, resta fermo, pertanto, quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01. 8. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria IDAM, almeno: a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza 9. Il servizio cloud supporta un meccanismo di cifratura di tipo Bring Your Own Key (BYOK), che consente all'Amministrazione di generare autonomamente, almeno la chiave principale di cifratura (root key), attraverso un HSM ospitato, alternativamente, presso: a. propria infrastruttura b. infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata c. infrastruttura di una terza parte scelta dall'Amministrazione. 10. Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 10 nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud. 11. Sono definite ed implementate procedure e misure tecniche misure per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi. 12. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1
PR.DS-3	2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti [SaaS] 3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto [SaaS]
ID.GV-1	3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governane strutturato 4. Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contentente almeno: a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6, b. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle polituche di sicurezza
PR.AC-3	5. Esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza

ID Requisito	Specifica Requisito
PR.AC-4	4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1
PR.IP-1	2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e il dispiegamento delle sole configurazioni adottate; b. l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza [SaaS] 3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni 4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità 5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile. 6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS] 7. È presente un sistema di gestione delle variazioni (in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].
PR.IP-12	3. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management 4. Il documento di cui al punto 1 della misura PR.IP-12 dovrà essere aggiornato su base semestrale.
PR.IP-2	1. Sono implementate linee guida e misure tecniche/organizzative per lo sviluppo sicuro del servizio cloud, in aderenza alle linee guida OWASP in merito alla sicurezza nello sviluppo del software (requisiti, progettazione, implementazione, test e verifica). Devono essere resi disponibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e alla Amministrazione i report sui test OWASP condotti, garantendo l'assenza di vulnerabilità di tipo "high" o "critical".
PR.IP-4	5. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno: a. le politiche di sicurezza adottate per il backup delle informazioni; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. 6. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

ID Requisito	Specifica Requisito
PR.IP-9	6. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal servizio cloud e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery. 7. Esiste un documento aggiornato di dettaglio contenente i piani di disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: a. le politiche e i processi impiegati per identificare le priorità degli eventi; b. le fasi di attuazione dei piani; c. i ruoli e le responsabilità del personale; d. i flussi di comunicazione e reportistica; e. il raccordo con il CSIRT Italia 8. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte. 9. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate. 10. I dispositivi critici per il funzionamento del servizio cloud sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore
PR.MA-1	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1. 3. Le attività di cui al punto 3 sono volte a verificare anche aspetti di sicurezza. 4. Gli aggiornamenti software sono consentiti solo da fonti pre-autorizzate. 5. Tutti i log relativi alle attività di manutenzione e aggiornamento sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività 6. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 3, 4, e 5
RS.MI-3	1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione 2. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.
PR.PT-5	1-bis. In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architettura ridondate di rete, di connettività, nonché applicative. b. esiste un sito di disaster recovery.
RC.RP-1	3. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

ID Requisito	Specifica Requisito
RS.RP-1	2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale. 3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate. 4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi 5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity. 6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza. 7. Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.
ID.RA-1	3. Le relazioni periodiche delle verifiche e dei test di cui al punto 1 devono contenere almeno: a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse; b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza; c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità. 4. Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.
ID.RA-5	4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno: a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento; b. le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DE.CM-8; c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-1	5. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity. 6. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono aggiornati, manutenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono impiegati anche per i fini di cui alla categoria DE.AE 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 3, 4 e 5; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

ID Requisito	Specifica Requisito
DE.CM-4	4. Sono configurati appositi software firewall su tutti i dispositivi. 5. I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox. 6. Gli strumenti tecnici di cui ai punti 1, 4 e 5 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PRAC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie IDAM, ID.GV, IDSC, PRAC e PRDS. 7. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-7	1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati. 2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete. 3. Gli strumenti tecnici di cui ai punti le 2 sono aggiornati, mantenuti e ben configurai, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PRAC e PRDS. 4. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 1 e 2; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-8	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration teste vulnerability assessment, prima della loro messa in esercizio. 2. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software. 3. Esiste un documento aggiornato recante la tipologia di penetration teste vulnerability assessment previsti. 4. Esiste un registro aggiornato dei penetration teste vulnerability assessment eseguiti corredato dalla relativa documentazione.
ID.SC-1	3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (Shared Security Responsibility Model-SSRM) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale. 4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione. 5. È fornita una chiara definizione in merito alla condivisione delle responsabilità.

ID Requisito	Specifica Requisito
ID.SC-2	1. In merito all'affidamento di forniture per i servizi cloud sono adottate misure in materia di sicurezza della catena di approvvigionamento cyber attraverso: a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione; b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore; c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del servizio cloud; d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno: i. della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza; ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo. 2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1.
ID.SC-3	1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.
ID.SC-4	1. Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata. 2. Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione. 3. È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio 4. Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente. 5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation.

Requisiti Dati Strategici

ID Requisito	Specifica Requisito
DE.AE-3	9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett a. b. c, d.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
PR.DS-1	13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio di cloud. Il soggetto rende disponibile l'elenco all'Amministrazione
PR.DS-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-5	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.AC-3	6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione. 7. È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati dello stesso. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati. 8. Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate
PR.AC-4	4. Tutte le attività privilegiate (es. installazione di aggiornamenti) e di accesso ai dati dell'Amministrazione da parte del personale del soggetto e di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitate ai soli casi essenziali.

ID Requisito	Specifica Requisito
PR.AC-5	3. Con riferimento ai censimenti di cui alla categoria IDAM, esiste un documento aggiornato di dettaglio contenente almeno: a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti; b. la descrizione delle reti segregate/segmentate; c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza; d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.
PR.AC-7	3. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla categoria ID.RA, contiene almeno: a. le modalità di autenticazione disponibili; b. la loro assegnazione alle categorie di transazioni
RC.IM-2	1. Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.MA-2	6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.
PR.MA-1	7. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite. 8. In base all'analisi del rischio, ogni aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo. 9. Il codice oggetto relativo agli aggiornamenti di cui al punto 3 viene custodito per almeno 24 mesi
PR.PT-1	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett a e b.
PR.PT-4	1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati. 2. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati. 3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 4. L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA. 5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE. 6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.

ID Requisito	Specifica Requisito
PR.PT-5	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.
DE.CM-7	5. Con riferimento alla sottocategoria IDAM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati. 6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate. 7. Gli strumenti tecnici di cui ai punti 5 e 6 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti 5 e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
ID.SC-1	6. Esiste un documento recante i processi di cui ai punti 1 e 2.
ID.SC-2	3. Si raccomanda, ove possibile e in relazione alla criticità di: a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto: i. della disponibilità del fornitore a condividere il codice sorgente; ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore; iii. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato all'interno dei beni e dei sistemi di information and communication technology; iv. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito. b. adottare processi e strumenti tecnici per: i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore; ii. acquisire il codice oggetto dai beni e sistemi di information and communication technology; iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito.
ID.SC-3	2. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.

16.2.5 *Requisiti ACN-Allegato C*

Requisiti per la qualificazione dei servizi Cloud per la Pubblica Amministrazione.

Servizi Cloud		
1	Ai fini della qualificazione di livello QC1 è richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali ordinari, ai sensi dell'articolo 3 del Regolamento.	Ai fini della qualificazione di livello QC1 sono richieste: - una certificazione ISO 9001 - Sistemi di Gestione per la Qualità (SGQ) per il servizio cloud oggetto di qualifica; - una certificazione ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle informazioni (SGSI) con estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019 per il servizio cloud oggetto di qualifica. In alternativa al suddetto requisito è possibile presentare certificazione Cloud Security Alliance - Star Level 2.
2	Ai fini della qualificazione di livello QC2 è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali critici, ai sensi dell'articolo 3 del Regolamento.	Ai fini della qualificazione di livello QC2 sono richieste: - un'autocertificazione che attesti la conformità allo standard ISO 22301- Business Continuity-Management System (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica; - un'autocertificazione che attesti la conformità allo standard ISO 20000-Service Management System per il servizio cloud oggetto di qualifica.
3	Ai fini della qualificazione di livello QC3 è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali strategici, ai sensi dell'articolo 3 del Regolamento	Ai fini della qualificazione di livello QC3 sono richieste: - una certificazione ISO 22301 - Business Continuity - Management System (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica; - una certificazione ISO/IEC 20000 (Service Management) per il servizio cloud oggetto di qualifica; - una certificazione Cloud Security Alliance - Star Level 2.

ID Caratteristica Specifica	Caratteristica specifica	ID Requisito	Nome	Specifica Requisito
S.1.1.	Requisiti in tema di controllo dei flussi	ID.AM-3	I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	2. Tutti i flussi per l'erogazione del servizio cloud sono soggetti a procedure di approvazione, di monitoraggio e di controllo concordati con l'Amministrazione
S.1.2.	Requisiti in tema di cifratura e gestione chiavi e autonomia operativa	PR.DS-1	I dati memorizzati sono protetti	14. Il servizio cloud supporta un meccanismo di cifratura di tipo Hold Your Own Key (HYOK), che consente all'Amministrazione la generazione e la gestione autonoma di tutte le chiavi di cifratura attraverso un HSM ospitato, alternativamente, presso: a. la propria infrastruttura b. un'infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata presso una terza parte scelta dall'Amministrazione 15. È garantito l'accesso esclusivo da parte dell'Amministrazione alle chiavi di cui al punto 1 e ai dati in chiaro dell'Amministrazione. 16. Il fornitore del servizio cloud mette a disposizione dell'Amministrazione un servizio di HSM in modalità dedicata. 17. Il soggetto è autonomo nella fornitura del servizio cloud, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.
S.1.3.	Requisiti in tema di verifica e controllo del personale	PR.IP-11	Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es. screening, deprovisioning)	1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato al servizio cloud o ai dati dell'Amministrazione. 2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato al servizio cloud o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.

Infrastruttura		
1	Ai fini della qualificazione di livello QI1 è richiesto il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali ordinari, ai sensi dell'articolo 3 del Regolamento	Ai fini della qualificazione di livello QI1 sono richieste: - una certificazione ISO 9001 - Sistemi di Gestione per la Qualità (SGQ) per l'infrastruttura digitale oggetto di qualifica - un'autocertificazione che attesti la conformità allo standard ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle informazioni, per l'infrastruttura digitale oggetto di qualifica
2	Ai fini della qualificazione di livello QI2 è richiesto il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali critici, ai sensi dell'articolo 3 del Regolamento	Ai fini della qualificazione di livello QI2 sono richieste: - un'autocertificazione che attesti la conformità allo standard ISO 22301 - Business Continuity - Management System (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica; - la certificazione ISO/IEC 27001:2013 - Sistema di gestione per la sicurezza delle informazioni per l'infrastruttura digitale oggetto di qualifica
3	Ai fini della qualificazione di livello QI3 è richiesto il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali strategici, ai sensi dell'articolo 3 del Regolamento	Ai fini della qualificazione di livello QI3 sono richieste: - una certificazione ISO 22301 - Business Continuity - Management System (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica.

ID Caratteristica Specifica	Caratteristica specifica	ID Requisito	Nome	Specifica Requisito
9.1.2	Requisiti in tema di verifica e controllo del personale	PR.IP-11	Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	1. Il soggetto rende disponibile all'Amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. 2. Il soggetto rende disponibile all'Amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'Amministrazione. L'Amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.

ALL 7

Da redigere su carta intestata dell'Amministrazione utente

Da redigere su carta intestata dell'Amministrazione utente

Spettabile
Polo Strategico Nazionale S.p.A.
Via G. Puccini 6
00198 - Roma

convenzione.psn@pec.polostrategiconazionale.it

Oggetto: Adesione alla Convenzione del 24.08.2022 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. Approvazione del Piano di Progetto dei fabbisogni 2023-000004733471009-PPdF-P1R1 del 01/02/2024 - Richiesta rilascio garanzia definitiva ai sensi dell'art. 15 dello schema di contratto di utenza.

In data _____ codesta Amministrazione ha approvato il Progetto del Piano dei fabbisogni di cui all'oggetto redatto dalla Società Polo Strategico Nazionale S.p.A (Concessionario) per usufruire dei servizi del Polo Strategico Nazionale come dettagliati nel Progetto stesso, deliberando, con delibera n. _____ del _____, di procedere alla sottoscrizione del relativo Contratto d'utenza.

Considerato che l'importo complessivo contrattuale che si intende stipulare è pari a euro 4.197.619,36 (€ _____ /00) al fine di completare l'iter per la sottoscrizione del Contratto di utenza, si richiede di produrre la garanzia definitiva, come prevista dall'art. 15 dello schema di Contratto di utenza per un importo pari al 4% dell'importo complessivo contrattuale e quindi pari a euro 167.904,77 (€ _____ /00).

Così come previsto dall'art. 15 dello schema di Contratto di utenza, l'importo della garanzia prestata in favore di codesta Amministrazione resta soggetta ad eventuali riduzioni di cui all'art. 103 del Codice intervenute prima o successivamente alla stipula.

In sede di stipula l'importo della garanzia è stato determinato tenendo conto delle riduzioni previste dal combinato disposto dell'art. 103, comma 1 e dell'art. 93, comma 7, del Codice dei contratti pubblici (D.Lgs. n. 50/2016 e ss.mm.ii.) in quanto il Concessionario, per il tramite dei propri soci, ha fornito prova del possesso delle certificazioni ISO14001 e ISO9001 che dà diritto alla riduzione del 60% dell'importo da garantire.

La garanzia definitiva prestata in favore di codesta Amministrazione dovrà avere 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.

Si prega pertanto di consegnare la garanzia definitiva entro 15 giorni lavorativi dal ricevimento della presente richiesta.