SISTEMA SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

N. 742 **del** 14/06/2024

OGGETTO: Adesione alla Convenzione sottoscritta col Dipartimento per la Trasformazione Digitale della Presidenza Consiglio dei Ministri. PNRR - Missione 1: Componente 1 - Investimento 1.1: "INFRASTRUTTURE DIGITALI" per il servizio di Migrazione al Polo Strategico Nazionale (CUP J81C23000670006). Importo complessivo € 22.833.649,06 iva inclusa.

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO PATRIMONIALE - UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE

Centro di Costo: BD07 L'Estensore:Dott.ssa SERENA SBRIGLIO Il presente Atto contiene dati sensibili

Il Dirigente e/o il Responsabile del procedimento, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attestano che l'atto è legittimo nella forma e nella sostanza.

Il Responsabile del Procedimento	UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE	DIPARTIMENTO TECNICO PATRIMONIALE
Ing. CLAUDIA CURCI	Dott. MASSIMILIANO COLTELLACCI	Ing. PAOLA BRAZZODURO
Firmatario: CLAUDIA CURCI Data: 10/06/2024 16:26:09 CEST	Firmatario: MASSIMILIANO COLTELLACCI Data: 10/06/2024 16:27:23 CEST	Firmatario: PAOLA BRAZZODURO Data: 11/06/2024 08:31:17 CEST

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta uno scostamento sfavorevole rispetto al budget economico assegnato come di seguito dettagliato per singolo conto:

Costo previsto	Eserciz.	CE/CP	Numero conto	Descrizione conto	Addetto al controllo	Scostamento
€456.163,17	2024	CE	504020298	Canoni di noleggio - area non sanitaria -STI	Dott. Massimiliano Coltellacci	No
€2.879.990,17	2024	CE	502020106	Servizi di assistenza informatica	Dott. Massimiliano Coltellacci	No

Risulta necessario procedere alle imputazioni contabili per i rispettivi anni di competenza come dettagliato in narrativa

Il Funzionario addetto al controllo di budget

Dott. MASSIMILIANO COLTELLACCI

Firmatario: MASSIMILIANO COLTELLACCI
Data: 10/06/2024 16:27:51 CEST

Il Dirigente della UOC Pianificazione Strategica, Programmazione e Controllo di Gestione con la sottoscrizione del presente atto attesta la coerenza della dichiarazione riferita alla spesa, di cui al presente provvedimento del "funzionario addetto al controllo del budget", rispetto alla delibera n. 176 del 13/02/2024

Il Dirigente della UOC Bilancio e Contabilità con la sottoscrizione del presente atto attesta la copertura economico/finanziaria della spesa di cui al presente provvedimento

Firmatario: STEFANIA DI CARLO
Data: 11/06/2024 17:13:10 CEST

Parere del Direttore Amministrativo Dr.ssa Roberta Volpini

Favorevole

Firmatario: MIRELLA PERACCHI
Data: 12/06/2024 10:27:01 CEST

(con motivazioni allegate al presente atto)
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 12/06/2024 17:39:50 CEST

(con motivazioni allegate al presente atto)
Non favorevole

Il presente provvedimento si compone di n.215 pagine di cui n.83 pagine di allegati

Il Commissario Straordinario
Dr. Giuseppe Quintavalle

Firmatario: GIUSEPPE QUINTAVALLE
Data: 14/06/2024 16:27:32 CEST

REGIONE LAZIO

IL DIRETTORE SOSTITUTO DELLA U.O.C. SISTEMI E TECNOLOGIE INFORMATICHE E DI COMUNICAZIONE

VISTA la deliberazione del Commissario Straordinario n. 1 del 1° gennaio 2016, con la quale si è provveduto a prendere atto dell'avvenuta istituzione dell'Azienda Sanitaria Locale Roma 1 a far data dal 1° gennaio 2016, come previsto dalla legge regionale n. 17 del 31.12.2015 e dal DCA n. 606 del 30.12.2015;

VISTO il Decreto del Presidente della Regione Lazio T00013 del 5 aprile 2023 con il quale è stato nominato Commissario Straordinario dell'Azienda Sanitaria Locale Roma 1, il dott. Giuseppe Quintavalle;

VISTO l'Atto di Autonomia Aziendale, approvato con deliberazione n. 1153 del 17/12/2019, recepito con DCA U00020 del 27/01/2020, pubblicato sul BURL del 30/01/2020 n. 9 con il quale, tra l'altro, è stato istituito il Dipartimento Tecnico Patrimoniale di cui fa parte la UOC Sistemi E Tecnologie Informatiche e di Comunicazione;

RICHIAMATA la Deliberazione n. 179 del 27/02/2020, avente ad oggetto "Atto aziendale dell'ASL Roma 1, approvato con Deliberazione n. 1153 del 17/12/2019 – Presa d'atto dell'esito positivo del procedimento di verifica regionale – Attuazione del nuovo modello organizzativo" la quale prevede l'attivazione del sopra citato Dipartimento e delle UU.OO.CC. nello stesso ricomprese;

VISTA la Delibera n. 347 del 08/07/2022 avente ad oggetto "*Sistema aziendale di deleghe e conseguente individuazione delle competenze nell'adozione degli atti amministrativi*" con la quale, tra l'altro, sono state individuate le competenze nell'adozione degli atti amministrativi;

VISTO il D.LGS. 36 del 31 marzo 2023 "Codice dei contratti pubblici" nel quale è previsto, all'art. 226 comma 2, che a decorrere dalla data in cui il codice acquista efficacia ai sensi dell'articolo 229, comma 2, le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi ai procedimenti in corso e che per procedimenti in corso, rientrano, tra gli altri, le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia;

VISTI 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, che 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;

il Decreto Legge 6 maggio 2021, n. 59, convertito con modificazioni dalla legge 1° luglio 2021, n. 101, recante "Misure urgenti relative al Fondo complementare al Piano Nazionale di Ripresa e Resilienza e altre misure urgenti per gli investimenti", che approva il Piano Nazionale per gli investimenti complementari finalizzato ad integrare con risorse nazionali gli interventi del Piano Nazionale di Ripresa e Resilienza e che, in ambito Salute, è focalizzato verso un ospedale sicuro e sostenibile e, in particolare, al miglioramento strutturale nel campo della sicurezza degli edifici ospedalieri;

il Decreto Legge n. 77 del 31 maggio 2021, convertito con modificazioni dalla legge n. 108 del 29 luglio 2021, recante "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure" nel quale, in ordine all'organizzazione della gestione del Piano Nazionale di Ripresa e Resilienza, vengono definiti i ruoli ricoperti dalle diverse amministrazioni coinvolte nonché le modalità di monitoraggio del Piano e del dialogo con le autorità europee e nel quale si prevedono misure di semplificazione che incidono in alcuni dei settori oggetto del PNRR al fine di favorirne la completa realizzazione;

DATTO ATTO che in data 14/03/2023 è stata pubblicato sulla piattaforma https://padigitale2026.gov.it l'Avviso "PNRR - MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.1 "INFRASTRUTTURE DIGITALI" e "INVESTIMENTO 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI" ASL/AO (MARZO 2023)", con scadenza alle ore 23:59 del 30/06/2023;

DATO ATTO che i finanziamenti di cui all'avviso sopra citato:

- sono collegati a quanto previsto per le PA in tema di migrazione al Cloud dei propri CED in relazione a quanto 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;

- sono relativi ai servizi necessari per le attività di migrazione al Cloud da parte delle ASL/AO e di gestione del primo anno di conduzione infrastrutturale;

- sono quantificati per ciascuna ASL/AO in ragione di parametri standard relativi al numero di assistiti/numero di posti letto, alla numerosità e alla classificazione ACN dei servizi da migrare in capo a ciascuna amministrazione, e automaticamente calcolati dalla piattaforma https://padigitale2026.gov.it in relazione a detti parametri;

DATO ATTO che l'ambito d'intervento di cui all'avviso di che trattasi, prevede la "full migration" dei servizi classificati dall'Ente, a meno delle deroghe previste dall'articolo 7 della Circolare AgID 1/2019 per i servizi di diagnostica clinica;

che per i finanziamenti all'avviso di cui sopra le ASL/AO sono Soggetti Attuatori;

DATO ATTO che la governance regionale dei progetti PNRR, tra cui rientra anche il progetto di migrazione al Cloud degli enti dell'SSR, è affidata alla Cabina di Regia costituita con Deliberazione di Giunta regionale n. 123 del 27/04/2023;

VISTE le note regionali protocollo reg. n. 0453681 del 26-04-2023 (acquisita al protocollo ASL con il n. 33404 del 26-04-2023), protocollo reg. n. 0505366 del 10-05-2023 (acquisita al protocollo ASL con il numero 37055 del 10-05-2023), protocollo reg. 0508997 del 11-05-2023 (acquisita al protocollo ASL con il numero 37285 del 11-05-2023) e protocollo ASL n. 38380 del 16-05-2023, con la quali la Regione Lazio ha:

- disposto la migrazione in Cloud verso l'operatore Polo Strategico Nazionale S.p.A. (di seguito anche abbrev. PSN) delle Aziende dell'SSR, ivi inclusi quelli direttamente gestiti al livello regionale;

• ha emanato le linee guida per la partecipazione all'Avviso di cui sopra;
• disposto la migrazione in Cloud verso l'operatore Polo Strategico Nazionale S.p.A. (di seguito anche abbrev. PSN) delle Aziende dell'SSR, ivi inclusi quelli direttamente gestiti al livello regionale;
• ha emanato le linee guida per la partecipazione all'Avviso di cui sopra;

DATO ATTO che il Dipartimento per la Trasformazione Digitale (di seguito anche abbrev. DTD) della Presidenza del Consiglio dei Ministri ha promosso la creazione del Polo Strategico Nazionale attraverso una Convenzione stipulata con la società di nuova costituzione Polo Strategico Nazionale S.p.A., partecipata da TIM, Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei;

che la Convenzione di cui sopra deriva da una "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 DTD;

che a seguito della procedura operata da Difesa Servizi S.p.A. è stato individuato l'operatore concessionario Polo Strategico Nazionale S.p.A.;

che la Convenzione di cui sopra prevede che le amministrazioni aderenti possano stipulare contratti, con una durata massima di 10 (dieci) anni, per effettuare la migrazione dei dati, servizi e applicazioni, nonché acquisire i servizi infrastrutturali cloud;

che la quantificazione economica dei servizi di migrazione e dei canoni per l'infrastruttura cloud per la migrazione al PSN sono stabiliti dalla Convenzione, in ragione dei prezzi definiti a seguito dell'aggiudicazione della relativa procedura aperta operata da Difesa Servizi S.p.A.;

che in data 29/05/2023 la ASL Roma 1 ha inoltrato candidatura all'avviso di che trattasi sulla piattaforma https://padigitale2026.gov.it, dando attuazione a quanto previsto dalle linee guida regionali così come sopra richiamate per la partecipazione all'avviso di che trattasi (Codice identificativo della candidatura: 85013);

che, i base ai parametri standard definiti dall'avviso e a quanto previsto dalle linee guida regionali in narrativa, a seguito di candidatura, la piattaforma https://padigitale2026.gov.it ha quantificato il finanziamento spettante alla ASL Roma 1 in € 7.812.432,00 :

che, per il perfezionamento della candidatura all'avviso in argomento, è stata richiesto dall'Ing. Claudia Curci dirigente ingegnere informatico presso la UOC STIC il codice CUP J81C23000670006 in qualità di RUP e inserito sulla piattaforma https://padigitale2026.gov.it nei tempi previsti dall'avviso stesso;

che, in esito alla candidatura all'avviso in parola, in data 22/08/2023, è stato notificato alla scrivente Azienda sulla piattaforma https://padigitale2026.gov.it il decreto di finanziamento n. 48-2/2023-PNRR e la stessa è stata ammessa per la linea di finanziamento 1.1 per un importo di € 7.812.432,00;

ALTRESI' che con giusta delibera del Commissario Straordinario n. 895 del 09/10/2023 la Scrivente Amministrazione ha preso atto del finanziamento di cui Decreto n. 48-2/2023-PNRR sopra citato;

DATO ATTO che, in riscontro alla nota regionale prot U.1159095.16-10-2023, acquisita al protocollo ASL con il numero 150082, 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 ASL Roma 1 ha trasmesso come richiesto i propri costi cessanti derivanti dal completamento della migrazione in cloud verso il PSN e il questionario sui servizi di sicurezza, nonché i costi relativi allo scenario alternativo;

ATTESTATO

che, con protocollo n. 49709, questa ASL ha trasmesso a firma del dall'Ing. Claudia Curci Dirigente della UOC 27/03/2024 il Piano dei Fabbisogni per la migrazione al PSN 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 del Piano dei Fabbisogni e tutti i documenti ad esso collegati per la contrattualizzazione;

che nel Piano dei Fabbisogni in parola sono stati inseriti, come da indicazioni regionali nelle riunioni di coordinamento con la Direzione ITD regionale, soltanto i servizi relativi alla migrazione degli applicativi al PSN e il dimensionamento dell'infrastruttura cloud necessaria per erogarli (canone annuale);

DATO ATTO che, in riscontro alla nota ASL prot. n. 49709, il PSN ha notificato a questa ASL a mezzo PEC in data 03/04/2024 (rif. protocollo ASL n. 52789) la presa in carico del Piano dei Fabbisogni così come trasmesso – codice presa in carico n. 2024-0000013664791004-PdF-P1R1;

DATO ATTO che, in esito alle richieste di chiarimento in data 9 maggio 2024 al Dipartimento della Transazione Digitale da questa Azienda per le operazioni di contrattualizzazione dell'operatore Polo Strategico Nazionale S.p.A., a seguito di mancata ricezione del PPDF dal PSN entro la scadenza del 18.05.24 alle ore 23:59, il Dipartimento della Transazione Digiale il 14 Maggio 2024 per le vie brevi autorizzava la ASL Roma 1 a procedere, tramite il portale PA Digitale 2026, alla posticipazione della data di contrattualizzazione al 17.06.24 alle ore 23:59 procedendo con la richiesta di proroga della scadenza di contrattualizzazione sulla piattaforma https://padigitale2026.gov.it al 17.06.24 alle ore 23:59

che in data 16/05/2024, sul portale PA Digitale 2026, è stata notificata alla Scrivente ASL l'approvazione della variazione di scadenza per la contrattualizzazione al 17.06.24 alle ore 23:59;

che in data 06/06/2024 a mezzo PEC, acquisita al protocollo ASL con il n. 90832, il PSN ha trasmesso il Progetto del Piano dei Fabbisogni – codice identificativo 2024-0000013664791004-PdF-P1R1, unitamente a seguenti allegati:

- Nota prot. 90832 del 06/06/2024;
- Progetto del Piano dei Fabbisogni;
- Schema di contratto;
- Allegato 6.2 Misure tecniche di sicurezza;
- Allegato 7 Richiesta fideiussione;

che è in corso la definizione il modello di documento di nomina del responsabile del trattamento dei dati con i rispettivi DPO in quanto non

vincolante ai fini della firma del contratto e al caricamento dello stesso in piattaforma PA Digitale 2026 entro i termini previsti dal finanziamento;

che la possibilità di fruire in modo efficace ed economico dei servizi di Disaster Recovery IT all'interno del PSN da parte di ASL Roma 1 è legata alla formalizzazione strategie ed azioni di continuità operativa dei processi clinici ed amministrativi ancora in stato di consolidamento all'interno della ASL Roma 1 con DPIA che dovrebbero fornire Piano di Recupero dal Disastro per permettere di dimensionare servizi tecnologici a garanzia della business continuity stessa;

che, con nota protocollo regionale n. U.1452284 del 14/12/2023, la Direzione Regionale Salute e Integrazione Sociosanitaria della Regione Lazio ha chiesto alla propria società in-house LAZIOcrea S.p.A. di coordinare dal punto di vista tecnico le progettualità e le attività di migrazione al PSN nel rispetto dei tempi e dei target previsti dal PNRR;

che la ASL Roma 1 ha inviato con nota prot. n. 91317 del 06/06/2024, alla Direzione Regionale Salute e Integrazione Sociosanitaria e alla Direzione Regionale per l'Innovazione Tecnologica e Trasformazione Digitale della Regione Lazioe LAZIOcrea S.p.A., il Progetto del Piano dei Fabbisogni – codice identificativo 2024-0000013664791004-PdF-P1R1;

che nella su indicata nota sono stati evidenziati:

- i costi esposti dal suddetto Progetto del Piano dei Fabbisogni, calcolati dall'operatore PSN in ragione dei prezzi di gara, rispetto agli importi finanziati a questa Azienda dal Decreto n. 48- 2/2023-PNRR;

- che gli atti previsti nella procedura operata da Difesa Servizi S.p.A. prevedono il pagamento dei corrispettivi nel rispetto delle specifiche previsioni contrattuali;

che il predetto Progetto del Piano dei Fabbisogni – codice identificativo 2024-0000013664791004-PdF-P1R1, così come trasmesso dal PSN, reca i seguenti importi economici:

- Servizi di Migrazione (Una Tantum nel primo anno di migrazione): € 2.123.044,45 IVA esclusa;
- Servizi Professionali: € 8.745.063,68 IVA esclusa;
- Canone annuo infrastruttura cloud (canone ricorrente dal 2024 al 2033): € 7.847.997,66 IVA esclusa;

che per quanto sopra il Q.E. complessivo a seguito della contrattualizzazione con PSN è il seguente:

Servizi PSN	Anno 1	Anno 2	Anno 3	Anno 4	Anno 5	Anno 6	Anno 7	Anno 8	Anno 9	Anno 10
Servizi di Migrazione	2.123.044,45 €									
Servizi Professionali	237.603,23 €	888.612,69 €	952.355,97 €	952.355,97 €	952.355,97 €	952.355,97 €	952.355,97 €	952.355,97 €	952.355,97 €	952.355,97 €
Canone annuo infrastruttura cloud	373.904,24 €	805.025,18 €	833.633,53 €	833.633,53 €	833.633,53 €	833.633,53 €	833.633,53 €	833.633,53 €	833.633,53 €	833.633,53 €
SOMMA PER ANNO	2.734.551,92 €	1.693.637,87 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €	1.785.989,50 €
IVA 22% PER ANNO	601.601,42 €	372.600,33 €	392.917,69 €	392.917,69 €	392.917,69 €	392.917,69 €	392.917,69 €	392.917,69 €	392.917,69 €	392.917,69 €
TOTALE PER ANNO	3.336.153,34 €	2.066.238,20 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €	2.178.907,19 €
TOTALE GENERALE 10 ANNI	18.716.105,79 €									
IVA 22%	4.117.543,27 €									
TOTALE 10 ANNI + IVA	22.833.649,06 €									

che si rende necessario procedere alle seguenti imputazioni contabili per i rispettivi anni di competenza, sulla base delle attuali indicazioni ricavate dalle Linee Guida del DTD per i Soggetti Attuatori individuati tramite avvisi pubblici a lump sum (pubblicati all'indirizzo https://innovazione.gov.it/italia-digitale-2026/attuazione-misure-pnrr/):

Conto	Servizio	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	Totale generale 10 anni
502020106- Servizi professionali(UT)	Servizi di Migrazione	2.123.044,45										2.123.044,45
502020106- Servizi professionali	Servizi Professionali	237.603,23	888.612,69	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	8.745.063,68
504020298-Canone	Canone annuo infrastruttura cloud	373.904,24	805.025,18	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	7.847.997,66
Totale per anno(IE)		2.734.551,92	1.693.637,87	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	18.716.105,79
Totale per anno(IC)		3.336.153,34	2.066.238,20	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	22.833.649,06

che a seguito dell'adozione del presente atto il CUP: J81C23000670006 - 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 - presenta la seguente situazione economica:

CUP J81C23000670006 M1C1 1.1 DIGITALIZZAZIONE DELLA PUBBLICA AMMINISTRAZIONE Misura Infrastrutture digitali (D.T.D. 48-3/2023-PNRR)				
BUDGET TOTALE ASSEGNATO				**7.812.432,00 €**
	Impegni anno 2024	**Impegni anno 2025**	**Impegni anno 2026**	**TOTALE**
BUDGET GIÀ IMPEGNATO	0,00 €	0,00 €	0,00 €	**0,00 €**
BUDGET IMPEGNATO CON IL PRESENTE ATTO	3.336.153,34 €	2.066.238,20 €	2.178.907,19 €	**7.581.298,73 €**
BUDGET RESIDUO				**231.140,27 €**

che il residuo di importo finanziato pari ad € 231.140,27 verrà utilizzato successivamente per l'acquisto del servizio housing di firewall fisici e relativa configurazione;

che parte dei servizi di migrazione è responsabilità dei fornitori dei servizi sui contratti già attivi presso questa azienda così come verrà meglio dettagliato nel successivo piano di migrazione a seguito della presente contrattualizzazione;

che si rinvia a successiva determinazione della struttura in attesa di approvazione del nuovo regolamento aziendale, l'imputazione e la liquidazione delle spese dovute per la corresponsione degli incentivi per Funzioni tecniche relativi alla presente procedura, per le fasi di programmazione, progettazione e predisposizionie degli atti di contrattualizzazione ed accantonamento per la fase di esecuzione;

che sono stati condotti accertamenti volti ad appurare l'esistenza di rischi da interferenza nell'esecuzione dell'appalto in oggetto e che, in base all'art. 26 c. 3-bis e dell'allegato XI del D.Lgs. n. 81/2008 come modificato dall'art. 32, comma 1, lettera a), Legge n. 98 del 2013, si prescinde dalla predisposizione del Documento Unico di Valutazione dei Rischi (DUVRI) in quanto trattasi di acquisizione di beni e servizi di natura intellettuale che non comportano rischi particolari per la sicurezza e la salute dei lavoratori;

che all'art. 21 Recesso del Contratto di Utenza è prevista la Rescissione decorsi i 36 mesi dalla data di avvio della gestione del servizio e che "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";

PRESO ATTO della richiesta di comando per incarico di funzione dirigenziale triennale dell'Ing. Claudia Curci presso altra Pubblica Amministrazione e del nulla osta rilasciato a far data dal 01/07/2024;

CONSIDERATO che, pertanto, risulta fondamentale con il presente atto effettuare contestualmente a far data dal 01/07/2024 la sostituzione dell'attuale Responsabile del Procedimento, Ing. Claudia Curci Dirigente di questa UOC, con il Dott. Massimiliano Coltellacci Direttore sostituto di questa UOC e conseguentemente si provvederà a seguire alla sostituzione in piattaforma CUP WEB per il CUP;

che la richiesta di CIG per procedure assoggettate al decreto legislativo n. 36/2023, pubblicate a partire dal 01/01/2024, avviene attraverso le piattaforme di approvvigionamento digitale certificate mediante interoperabilità con i servizi erogati dalla PCP attraverso la Piattaforma Digitale Nazionale Dati (PDND);

RICHIAMATA la delibera ANAC n. 582 del 13 dicembre 2023 avente ad oggetto Adozione comunicato relativo all'avvio del processo di digitalizzazione nella quale è previsto l'utilizzo della Utilizzo dell'interfaccia web della Piattaforma contratti pubblici per l'acquisizione di CIG per adesione ad accordi quadro e convenzioni i cui bandi siano stati pubblicati entro il 31/12/2023 con o senza successivo confronto competitivo;

DATO ATTO quindi che il Codice Identificativo di Gara (CIG) verrà acquisito mediante la PCP, successivamente al perfezionamento del presente atto;

RITENUTO per tutto quanto sopra in narrativa di dover procedere all'adesione alla Convenzione per la migrazione al Cloud verso l'operatore Polo Strategico Nazionale S.p.A., al fine di ottemperare agli obiettivi regionali così come sopra esposti in narrativi e nei tempi richiesti dall'Avviso "PNRR - MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.1 "INFRASTRUTTURE DIGITALI" e "INVESTIMENTO 1.2 ABILITAZIONE AL CLOUD PER LE

PA LOCALI" ASL/AO (MARZO 2023)" e dal relativo Decreto di finanziamento n. 48-2/2023-PNRR;

ATTESTATO che il presente provvedimento a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge n. 241/1990 e successive modifiche ed integrazioni;

PROPONE

Per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire alla Convenzione sottoscritta col Dipartimento per la Trasformazione Digitale della Presidenza Consiglio dei Ministri. PNRR - Missione 1: Componente 1 - Investimento 1.1: "INFRASTRUTTURE DIGITALI" per il servizio di Migrazione al Polo Strategico Nazionale (CUP J81C23000670006). Importo complessivo € 22.833.649,06 iva inclusa;

di approvare il Progetto dei Fabbisogni codice identificativo 2024-0000013664791004-PdF-P1R1 così come trasmesso dal PSN, unitamente agli allegati:

- Nota prot. 90832 del 06/06/2024;
- Progetto del Piano dei Fabbisogni
- Schema di contratto;
- Allegato 6.2 Misure tecniche di sicurezza;
- Allegato 7 Richiesta fideiussione

di dare atto che la spesa totale derivante dall'adozione del presente provvedimento, pari ad 22.834.019,36 iva inclusa, è da imputare sui conti di esercizio e come di seguito dettagliato - Finanziata mediante PNRR – M1C1 1.1 Digitalizzazione della Pubblica Amministrazione Misura Infrastrutture digitali (D.T.D. 48-3/2023-PNRR), cosi come di seguito specificato:

Conto	Servizio	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	Totale generale 10 anni
502020106- Servizi professionali(UT)	Servizi di Migrazione	2.123.044,45										2.123.044,45
502020106- Servizi professionali	Servizi Professionali	237.603,23	888.612,69	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	8.745.063,68
504020298-Canone	Canone annuo infrastruttura cloud	373.904,24	805.025,18	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	7.847.997,66
Totale per anno(IE)		2.734.551,92	1.693.637,87	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	18.716.105,79
Totale per anno(IC)		3.336.153,34	2.066.238,20	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	22.833.649,06

di effettuare a far data dal 01/07/2024 la sostituzione dell'attuale Responsabile del Procedimento, Ing. Claudia Curci Dirigente della UOC Sistemi e Tecnologie Informatiche e di Comunicazione, con il Dott. Massimiliano Coltellacci Direttore sostituto della UOC Sistemi e Tecnologie Informatiche e di Comunicazione; di nominare DEC della presente procedura Dott. Pio Pucci, afferente alla UOC Sistemi e Tecnologie Informatiche e di Comunicazione;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla

protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile del procedimento	Il Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione	Il Direttore Dipartimento Tecnico Patrimoniale
Ing. Claudia Curci	Dott. Massimiliano Coltellacci	Ing. Paola Brazzoduro
FIRMATO DIGITALMENTE	*FIRMATO DIGITALMENTE*	*FIRMATO DIGITALMENTE*

IL COMMISSARIO STRAORDINARIO

IN VIRTÚ dei poteri previsti:

- dall'art. 3 del D. Lgs 502/1992 e ss.mm.ii;
- dall'art. 8 della L.R. n. 18/1994 e ss.mm.ii;

nonché delle funzioni e dei poteri conferitigli con Decreto del Presidente della Regione Lazio n. T00013 del 5 aprile 2023;

Letta la proposta di delibera sopra riportata presentata dal Dirigente Responsabile dell'Unità in frontespizio indicata;

PRESO ATTO che il Direttore della Struttura proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge 241/1990 e successive modifiche ed integrazioni;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario riportati in frontespizio;

DELIBERA

di adottare la proposta di deliberazione avente per oggetto "Adesione alla Convenzione sottoscritta col Dipartimento per la Trasformazione Digitale della Presidenza Consiglio dei Ministri. PNRR - Missione 1: Componente 1 - Investimento 1.1: "INFRASTRUTTURE DIGITALI" per il servizio di Migrazione al Polo Strategico Nazionale (CUP J81C23000670006). Importo complessivo € 22.833.649,06 iva inclusa." e conseguentemente, per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire alla Convenzione sottoscritta col Dipartimento per la Trasformazione Digitale della Presidenza Consiglio dei Ministri. PNRR - Missione 1: Componente 1 - Investimento 1.1: "INFRASTRUTTURE DIGITALI" per il servizio di Migrazione al Polo Strategico Nazionale (CUP J81C23000670006). Importo complessivo € 22.833.649,06 iva inclusa;

di approvare il Progetto dei Fabbisogni codice identificativo 2024-0000013664791004-PdF-P1R1 così come trasmesso dal PSN, unitamente agli allegati:

- Nota prot. 90832 del 06/06/2024;
- Progetto del Piano dei Fabbisogni
- Schema di contratto;
- Allegato 6.2 Misure tecniche di sicurezza;
- Allegato 7 Richiesta fideiussione

di dare atto che la spesa totale derivante dall'adozione del presente provvedimento, pari ad 22.834.019,36 iva inclusa, è da imputare sui conti di esercizio e come di seguito dettagliato - Finanziata mediante PNRR – M1C1 1.1 Digitalizzazione della Pubblica Amministrazione Misura Infrastrutture digitali (D.T.D. 48-3/2023-PNRR), cosi come di seguito specificato:

Conto	Servizio	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	Totale generale 10 anni
502020106- Servizi professionali(UT)	Servizi di Migrazione	2.123.044,45										2.123.044,45
502020106- Servizi professionali	Servizi Professionali	237.603,23	888.612,69	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	952.355,97	8.745.063,68
504020298-Canone	Canone annuo infrastruttura cloud	373.904,24	805.025,18	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	833.633,53	7.847.997,66
Totale per anno(IE)		2.734.551,92	1.693.637,87	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	1.785.989,50	18.716.105,79
Totale per anno(IC)		3.336.153,34	2.066.238,20	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	2.178.907,19	22.833.649,06

di effettuare a far data dal 01/07/2024 la sostituzione dell'attuale Responsabile del Procedimento, Ing. Claudia Curci Dirigente della UOC Sistemi e Tecnologie Informatiche e di Comunicazione, con il Dott. Massimiliano Coltellacci Direttore sostituto della UOC Sistemi e Tecnologie Informatiche e di Comunicazione; di nominare DEC della presente procedura Dott. Pio Pucci, afferente alla UOC Sistemi e Tecnologie Informatiche e di Comunicazione;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile della struttura proponente provvederà all'attuazione della presente deliberazione curandone altresì la relativa trasmissione agli uffici/organi rispettivamente interessati.

Il COMMISSARIO STRAORDINARIO
Dr. Giuseppe Quintavalle
FIRMATO DIGITALMENTE

Da:	Per conto di: convenzione.psn@pec.polostrategiconazionale.it <posta-certificata@telecompost.it>
Inviato:	mercoledì 05 giugno 2024 14.53
A:	protocollo@pec.aslroma1.it
CC:	pierluigi.lamantia@polostrategiconazionale.it, massimiliano.chirico@polostrategiconazionale.it
Oggetto:	POSTA CERTIFICATA: Invio del Progetto del Piano dei Fabbisogni n. 2024-0000013664791004-PPdF-P1R1 ai sensi dell?art. 18 della Convenzione sottoscritta tra PSN S.p.A. e il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri in data 24 agosto 2022.
Allegati:	2024-0000013664791004-PPdF-P1R1 ASL RM1.pdf;4. PSN_master contratto utenza v.22.4.24 v.2_recesso 36M_ASLRM1_definitivo.docx;All_7 richiesta fideiussione PA ex.docx;All_6.2 misure tecniche sicurezza.pdf;All_6.1 Nomina Responsabile del Trattamento -.docx

Spettabile Azienda Sanitaria Locale Roma 1,
Vi trasmettiamo in allegato alla presente comunicazione il Progetto del Piano dei Fabbisogni, identificato dal codice n. 2024-0000013664791004-PPdF-P1R1 (di seguito il “Codice”) contenente la proposta tecnico-economica per la fornitura di Servizi del Polo Strategico Nazionale, redatto in conformità alle richieste da Voi espresse nel Piano dei Fabbisogni ricevuto in data 27/03/2024. Vi informiamo che tutte le eventuali future comunicazioni relative al Progetto del Piano dei Fabbisogni formalizzato dovranno contenere il riferimento al Codice e dovranno essere trasmesse a mezzo PEC al seguente indirizzo: convenzione.psn@pec.polostrategiconazionale.it.

Come previsto dall’art. 18, comma 3 della Convenzione (disponibile su www.polostrategiconazionale.it), si ricorda che è Vostra facoltà presentare osservazioni al Progetto del Piano dei Fabbisogni nel termine di 10 giorni solari dalla ricezione della presente comunicazione. In tale caso, si applicheranno le disposizioni di cui all’art. 18, commi da 3 a 6 della Convenzione.

Ai fini della stipula del Contratto d’Utenza Vi ricordiamo che è necessario:

1. inviare, entro 10 giorni solari dalla ricezione della presente, a mezzo PEC all’indirizzo convenzione.psn@pec.polostrategiconazionale.it, una comunicazione di accettazione del Progetto del Piano dei Fabbisogni e una richiesta di rilascio della garanzia definitiva (secondo il modello di seguito allegato sub Allegato 1 debitamente compilato e sottoscritto);
2. compilare, firmare digitalmente (con firma visibile in formato PAdES) e inviare a mezzo PEC all’indirizzo convenzione.psn@pec.polostrategiconazionale.it i documenti di seguito elencati:

- Allegato 2: il Contratto d’Utenza con il CIG derivato assegnato al Contratto d’Utenza (CIG della Convenzione è 9066973ECE);
- Allegato 3: il Progetto del Piano dei Fabbisogni;
- Allegato 4: il template standard per la Nomina a Responsabile del Trattamento dei dati sub Allegato E al Contratto d’Utenza comprensivo del Manuale Tecnico Misure di Sicurezza.

In ottemperanza alla vigente normativa in materia di sicurezza sui luoghi di lavoro, si richiede di trasmettere a mezzo PEC (all’indirizzo convenzione.psn@pec.polostrategiconazionale.it) le informazioni di cui alla lettera b) del primo comma dell’art. 26 TUSL INFORMATIVA DEI RISCHI DI SEDE contenente le informazioni in merito alle norme comportamentali, restando inteso che la mancata trasmissione di tali informazioni non consentirà l’erogazione dei Servizi in presenza. Le attività svolte da PSN e dai soci sono configurabili di tipo intellettuali, non ricadenti sotto DUVRI, qualora le attività svolte non si configurino come precedentemente descritto l’Amministrazione provvederà a fornire DUVRI.

Per ogni eventuale chiarimento potrete rivolgerVi al referente commerciale di PSN in copia nella presente comunicazione.

Cordiali saluti
Polo Strategico Nazionale S.p.A.

Polo Strategico Nazionale

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 1

PSN-SDE-CONV22-001-2024-0000013664791004-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	04/06/2024

Tabella 1: Informazioni Documento

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

Tabella 2: Autore

Revisione:	
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 AZIENDA SANITARIA LOCALE ROMA 1
  - Massimiliano Coltellacci
  - Email: massimiliano.coltellacci@aslroma1.it
- Referente Tecnico AZIENDA SANITARIA LOCALE ROMA 1
  - Claudia Curci
  - Email: claudia.curci@aslroma1.it
- Referente Sicurezza AZIENDA SANITARIA LOCALE ROMA 1
  - Stefano Scaramuzzino
  - Email: stefano.scaramuzzino@aslroma1.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 *AZIENDA SANITARIA LOCALE ROMA 1* di seguito anche ASL RM1 o Amministrazione, sulla base delle esigenze emerse dal Piano dei Fabbisogni (ID 2024-0000013664791004-PPdF-P1R1).

2 AMBITO

La migrazione in cloud dell'infrastruttura e dei servizi della ASL RM1 rappresenta un processo complesso che richiede il soddisfacimento di vari requisiti cruciali per garantire una transizione efficace e sicura. In primo luogo, questa migrazione seguirà il modello Lift&Shift, che comporterà lo spostamento delle macchine virtuali (VM) dall'ambiente on premises all'ambiente cloud. Questo spostamento si avvarrà di appositi strumenti di migrazione, come tool automatizzati, export/import di immagini VM o reinstallazione, laddove non sia disponibile un'alternativa.

Durante l'intero processo di migrazione il Polo Strategico Nazionale (PSN) fornirà servizi infrastrutturali, sistemistici e applicativi necessari per la migrazione, in linea con i requisiti specificati nel documento. Ciò includerà l'implementazione e la gestione dell'infrastruttura richiesta per supportare le applicazioni e i servizi durante la migrazione. Il PSN dovrà altresì effettuare la gestione dei team di lavoro e quindi dell'intero progetto di migrazione.

L'Amministrazione possiede attualmente un'infrastruttura on premises basata su tecnologie eterogenee su cui vengono eseguite applicazioni critiche e ordinarie implementate e gestite da fornitori applicativi diversi. Date le scadenze e il ruolo di primo piano che ricoprono i servizi oggetto di migrazione, il PSN intende allestire un team di lavoro con profili ed esperienze adeguate al fine id garantire all'Amministrazione il minimo impatto sulla fruizione dei servizi, sia durante le fasi più critiche di migrazione che durante l'intero arco temporale di permanenza dell'Amministrazione stessa all'interno del PSN.

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 infrastrutturali
- Servizi di migrazione in modalità Lift & Shift per le componenti applicative conformi ai requisiti minimi PSN e con preliminare aggiornamento dei sistemi operativi per le componenti applicative legacy

La modalità di migrazione prevista, ad oggi, è quella descritta dalla Modalità A - Trasferimento in sicurezza dell'infrastruttura IT:

Servizio dell'Amministrazione	Tipo di migrazione
ANAGRAFE NAZIONALE ASSISTIBILI - ANAGRAFE NAZIONALE ASSISTIBILI	Modalità A
ASSISTENZA A PARTICOLARI CATEGORIE - ASSISTENZA A PARTICOLARI CATEGORIE	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA FARMACEUTICA	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA RESIDENZIALE E SEMI-RESIDENZIALE	Modalità A

ASSISTENZA DISTRETTUALE - ASSISTENZA SOCIOSANITARIA AI MINORI, ALLE DONNE, ALLE COPPIE, ALLE FAMIGLIE	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA SPECIALISTICA AMBULATORIALE	Modalità A
ASSISTENZA DISTRETTUALE - CURE DOMICILIARI (ANCHE PALLIATIVE)	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA INTEGRATIVA	Modalità A
ASSISTENZA DISTRETTUALE - PERCORSI ASSISTENZIALI INTEGRATI	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA PROTESICA	Modalità A
ASSISTENZA DISTRETTUALE - ASSISTENZA SANITARIA DI BASE	Modalità A
ASSISTENZA DISTRETTUALE - CONTINUITÀ ASSISTENZIALE	Modalità A
ASSISTENZA DISTRETTUALE - EMERGENZA SANITARIA TERRITORIALE	Modalità A
ASSISTENZA OSPEDALIERA - ASSISTENZA SPECIALISTICA AMBULATORIA LE	Modalità A
ASSISTENZA OSPEDALIERA - ATTIVITÀ DIAGNOSTICA	Modalità A
ASSISTENZA OSPEDALIERA - ATTIVITÀ TRASFUSIONALI	Modalità A
ASSISTENZA OSPEDALIERA - DAY HOSPITAL	Modalità A
ASSISTENZA OSPEDALIERA - DAY SURGERY	Modalità A
ASSISTENZA OSPEDALIERA - RIABILITAZIONE E LUNGODEGENZ A POST ACUZIE	Modalità A
ASSISTENZA OSPEDALIERA - RICOVERO ORDINARIO PER ACUTI	Modalità A
ASSISTENZA OSPEDALIERA - PRONTO SOCCORSO	Modalità A
EDUCAZIONE CONTINUA IN MEDICINA - EDUCAZIONE CONTINUA IN MEDICINA	Modalità A
FASCICOLO SANITARIO REGIONALE - FASCICOLO SANITARIO REGIONALE	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - ATTIVITÀ MEDICO LEGALI PER FINALITÀ PUBBLICHE	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA – SORVEGLIANZA, PREVENZIONE E CONTROLLO DELLE MALATTIE INFETTIVE E PARASSITARIE, INCLUSI I PROGRAMMI VACCINALI	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - SICUREZZA ALIMENTARE – TUTELA DELLA SALUTE DEI CONSUMATORI	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - TUTELA DELLA SALUTE E DELLA SICUREZZA DEGLI AMBIENTI APERTI E CONFINATI	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - SORVEGLIANZA E PREVENZIONE DELLE MALATTIE CRONICHE, INCLUSI LA PROMOZIONE DI STILI DI VITA SANI ED I PROGRAMMI ORGANIZZATI DI SCREENING; SORVEGLIANZA E PREVENZIONE NUTRIZIONALE	Modalità A
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA - SALUTE ANIMALE E IGIENE URBANA VETERINARIA	Modalità A

RETI DI PATOLOGIA - RETI DI PATOLOGIA	Modalità A
RISCHIO CLINICO - RISCHIO CLINICO	Modalità A
SERVIZI DI FUNZIONAMENTO - ACQUISTI	Modalità A
SERVIZI DI FUNZIONAMENTO - CONTABILITÀ, BILANCIO E CONTROLLO	Modalità A
SERVIZI DI FUNZIONAMENTO - GESTIONE DOCUMENTALE	Modalità A
SERVIZI DI FUNZIONAMENTO - PERSONALE	Modalità A
SERVIZI DI FUNZIONAMENTO - PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	Modalità A
SERVIZI DI FUNZIONAMENTO - PROTOCOLLO	Modalità A
SERVIZI INFORMATIVI - COMUNICAZIO NE ISTITUZIONALE WEB E OPEN DATA	Modalità A
SERVIZI INFORMATIVI - RAPPORTI CON L'UTENZA - URP	Modalità A

Al fine di completare il quadro descrittivo delle applicazioni oggetto di migrazione su PSN, si riporta di seguito la classificazione secondo ACN del parco servizi ad oggi operativi presso l'Amministrazione.

Categoria	Nome Servizio	Descrizione	Classificazione ACN
ANAGRAFE NAZIONALE ASSISTIBILI	ANAGRAFE NAZIONAL E ASSISTIBILI	Gestione integrazione/conferimento dati verso l'Anagrafe nazionale degli assistititi (ANA) istituita dall'articolo 62-ter del CAD, nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze in attuazione di quanto disposto dall'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326 (Sistema Tessera Sanitaria)	CRITICO
ASSISTENZA A PARTICOLARI CATEGORIE	ASSISTENZ A A PARTICOL ARI CATEGORI E	Assistenza a particolari categorie quali: - invalidi, - affetti da malattie rare, - affetti da malattie croniche e invalidanti, - affetti da fibrosi cistica, - nefropatici cronici in trattamento dialitico, - affetti da morbo di hansen, - persone con infezioni da hiv/aids, - soggetti detenuti ed internati in istituti penitenziari e minori sottoposti a provvedimento penale, - donne in stato di gravidanza e tutela	CRITICO

		della maternità, - persone con disturbi dello spettro autistico, - cittadini italiani residenti in italia autorizzati alle cure all'estero, - cittadini stranieri iscritti al ssn, - cittadini stranieri non iscritti al ssn non in regola con il permesso di soggiorno.	
ASSISTENZA DISTRETTUALE	ASSISTENZA FARMACEUTICA	erogazione dei medicinali attraverso le farmacie convenzionate e le farmacie direttamente gestite dalle ASL/AUSL e dalle AO;	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA RESIDENZIALE E SEMI-RESIDENZIALE	Accesso a strutture residenziali e semiresidenziali a seguito di valutazione multidisciplinare successiva ad una richiesta da parte del MMG/PLS oppure da parte dell'Assistente Sociale del Comune di Residenza. Comprende: -Assistenza sociosanitaria residenziale e semiresidenziale alle persone non autosufficienti -Assistenza sociosanitaria residenziale alle persone nella fase terminale della vita -Assistenza sociosanitaria (anche semiresidenziale e residenziale) ai minori con disturbi in ambito neuropsichiatrico e del neurosviluppo -Assistenza sociosanitaria (anche semiresidenziale e residenziale) alle persone con disturbi mentali -Assistenza sociosanitaria (anche semiresidenziale e residenziale) alle persone con disabilità -Assistenza sociosanitaria (anche semiresidenziale e residenziale) alle persone con dipendenze patologiche	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA SOCIOSANITARI A AI MINORI , ALLE DONNE, ALLE COPPIE, ALLE FAMIGLIE	Assistenza sociosanitaria a minori, donne, coppie e famiglie nell'ambito dell'assistenza distrettuale, domiciliare e territoriale ad accesso diretto. Comprende le prestazioni - anche domiciliari - mediche specialistiche, diagnostiche e terapeutiche, ostetriche, psicologiche e psicoterapeutiche, e riabilitative, mediante l'impiego di metodi e strumenti basati sulle piu' avanzate evidenze scientifiche, necessarie ed appropriate in vari ambiti di attività.	CRITICO
ASSISTENZA OSPEDALIERA	ASSISTENZA SPECIALISTI	Insieme delle prestazioni terapeutiche erogate dai medici ospedalieri negli ambulatori ospedalieri pubblici	CRITICO

	CA AMBULATORIA LE		
ASSISTENZA DISTRETTUALE	CURE DOMICILIARI (ANCHE PALLIATIVE)	Assistenza sanitaria a domicilio a persone non autosufficienti o in condizioni di fragilità, attraverso l'erogazione delle prestazioni mediche, riabilitative, infermieristiche e di aiuto infermieristico necessarie e appropriate in base alle specifiche condizioni di salute della persona (Art. 22 del dPCM 12 gennaio 2017)	CRITICO
ASSISTENZA DISTRETTUALE	PERCORSI ASSISTENZIALI INTEGRATI	presa in carico totale dell'assistito, dal suo primo contatto con il SSN al trattamento terapeutico dopo la diagnosi, gestione dell'iter organizzativo, delle fasi e le procedure di presa in carico del paziente, interventi multiprofessionali conseguenti.	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA INTEGRATIVA	erogazione di dispositivi medici (pannoloni, cateteri, cannule, medicazioni, presidi per diabetici, ecc.) e di alimenti particolari (prodotti senza glutine, prodotti aproteici, latte artificiale, ecc.) a specifiche categorie di pazienti;	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA PROTESICA	erogazione di protesi, ortesi, ausili tecnologici e dispositivi medici a persone con disabilità permanenti;	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA SANITARIA DI BASE	assistenza erogata dai medici di medicina generale e dai pediatri di libera scelta;	CRITICO
ASSISTENZA DISTRETTUALE	CONTINUITÀ ASSISTENZIALE	assistenza di base nelle ore notturne e nei giorni prefestivi e festivi, e l'assistenza ai turisti;	CRITICO
ASSISTENZA DISTRETTUALE	EMERGENZA SANITARIA TERRITORIALE	servizio di stabilizzazione delle condizioni del malato e di trasporto presso il presidio ospedaliero, coordinata dalla Centrale operativa 118, e assistenza sanitaria in occasione di maxi emergenze, eventi o manifestazioni;	CRITICO
ASSISTENZA DISTRETTUALE	ASSISTENZA SPECIALISTICA AMBULATORIALE	prestazioni diagnostiche e terapeutiche erogate dai (o sotto la responsabilità clinica dei) medici specialisti ambulatoriali negli ambulatori e nei laboratori pubblici o privati accreditati, territoriali o ospedalieri (gli ambulatori e i laboratori specialistici svolgono attività distrettuale anche se fisicamente collocati all'interno di strutture ospedaliere);	CRITICO

ASSISTENZA OSPEDALIERA	ATTIVITÀ DIAGNOSTICA	L'attività di diagnostica strumentale (RX, TAC, RM, scintigrafia, ecografia, ECG, EEG, gastroscopia, colonscopia, artroscopia, audiometria, ecc.) e di Laboratorio (Chimica clinica; Microbiologia; Virologia; Anatomia e istologia patologica; Genetica; Immunoematologia) per i cittadini ricoverati che nell'ambito delle Prestazioni Territoriali	CRITICO
ASSISTENZA OSPEDALIERA	ATTIVITÀ TRASFUSIONALI	L'art. 47 del DPCM 12 gennaio 2017 prevede che il SSN garantisce in materia di attività trasfusionale i servizi e le prestazioni individuati dalla Legge 219/2005. Le trasfusioni rappresentano una terapia salvavita in varie circostanze quali, ad esempio, eventi traumatici, come gli incidenti, interventi chirurgici, in caso di patologie croniche, per esempio nelle anemie congenite come la talassemia, per il superamento di stati critici dovuti a malattie del sangue (leucemia)	CRITICO
ASSISTENZA OSPEDALIERA	DAY HOSPITAL	Forma di assistenza detta anche "ricovero diurno", garantita dal Servizio sanitario nazionale, che permette al paziente di usufruire di cure ospedaliere nell'arco di uno o più ricoveri programmati (tutti di durata inferiore a un giorno e senza pernottamento) per lo svolgimento di accertamenti diagnostici, visite specialistiche e terapie. La permanenza in ospedale è limitata al tempo strettamente necessario e, completate le cure, il paziente torna al proprio domicilio avendo la possibilità di continuare, per quanto possibile, le attività quotidiane	CRITICO
ASSISTENZA OSPEDALIERA	DAY SURGERY	Modalità clinico-organizzativa per effettuare interventi chirurgici o procedure diagnostiche e/o terapeutiche invasive, in regime di ricovero limitato alle sole ore del giorno, in anestesia generale, loco-regionale o locale. Ciò consente un precoce ritorno al proprio ambiente familiare, riducendo al minimo il disagio generato dall'ospedalizzazione	CRITICO
ASSISTENZA OSPEDALIERA	RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	Processo di riabilitazione nel corso del quale si porta una persona con disabilità a raggiungere il miglior livello di autonomia possibile sul piano fisico, funzionale, sociale, intellettivo e relazionale, con la minor restrizione delle sue scelte operative, pur nei limiti della sua menomazione.	CRITICO
ASSISTENZA OSPEDALIERA	RICOVERO ORDINARIO	Reti assistenziali ospedaliere per l'assistenza a pazienti acuti che forniscono indicazioni operative rivolte sia agli aspetti propriamente clinici della	CRITICO

	PER ACUTI	gestione della patologia, sia alle esigenze organizzative sottese al soddisfacimento del bisogno complessivo di salute, spostando il focus degli operatori e dell'intero sistema dalla visione incentrata sul "prodotto", cioè sulla singola prestazione erogata, alla visione incentrata sul "risultato", cioè sulla ricaduta in termini di salute della popolazione	
ASSISTENZA OSPEDALIERA	PRONTO SOCCORSO	Funzione di pronto soccorso ospedaliero garantita all'interno della rete ospedaliera dell'emergenza, alla costituzione della quale concorrono strutture di diversa complessità assistenziale ed organizzativa, poste tra loro in correlazione funzionale integrata, secondo il modello hub and spoke. Prescrive ricoveri. E' attiva 24 ore su 24, 365 giorni all'anno.	CRITICO
EDUCAZIONE CONTINUA IN MEDICINA	EDUCAZIONE CONTINUA IN MEDICINA	Sistema ECM (Educazione Continua in Medicina) che comprende l'insieme organizzato e controllato di tutte quelle attività formative, sia teoriche che pratiche, promosse da chiunque lo desideri con lo scopo di mantenere elevata e al passo con i tempi la professionalità degli operatori di sanità. Tale sistema è stato istituzionalizzato in Italia con d.lgs 30 dicembre 1992, n. 502 così come modificato dal d.lgs. 19 giugno 1999, n. 229.	ORDINARIO
FASCICOLO SANITARIO REGIONALE	FASCICOLO SANITARIO REGIONALE	Gestione integrazione/conferimento dati verso Fascicolo Sanitario Elettronico Regionale. Il Fascicolo Sanitario Elettronico è l'insieme dei dati, dei documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi.	CRITICO
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	ATTIVITÀ MEDICO LEGALI PER FINALITÀ PUBBLICHE	Attività che la finalità di promuovere la cultura della sicurezza nei trattamenti sanitari, mediante una ottimale gestione del rischio, in particolare di quello clinico, anche per fronteggiare il grave problema della conflittualità fra cittadini, professionisti della salute e ASL/AUSL o AO	ORDINARIO
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	SORVEGLIANZA, PREVENZIONE E CONTROLLO DELLE MALATTIE INFETTIVE E PARASSITARIE	Tutte le attività volte a soddisfare il Piano Nazionale Prevenzione Vaccinale e garantire la corretta valutazione delle coperture vaccinali, utile sia a monitorare l'attuazione dei programmi vaccinali in atto su tutto il territorio nazionale, coerentemente con il calendario vaccinale nazionale vigente, sia a fornire informazioni agli organi nazionali, comunitari ed internazionali	CRITICO

	, INCLUSI I PROGRAMMI VACCINALI	nell'ambito dello svolgimento di funzioni e compiti correlati alla tutela della salute, anche mediante l'elaborazione di indicatori a fini comparativi.	
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	SICUREZZA ALIMENTARE – TUTELA DELLA SALUTE DEI CONSUMATORI	Tutte le attività per la prevenzione delle contaminazioni ambientali e tecnologiche degli alimenti e dei mangimi, per contrastare l'insorgenza di fenomeni di antibiotico-resistenza tramite la lotta all'abuso di antibiotici e di farmaci antimicrobici in ambito zootecnico, per il controllo dell'insorgenza delle zoonosi nuove e riemergenti e per la promozione di una nuova modalità di realizzazione del rapporto uomo-animale, che tenga conto della evoluta sensibilità della popolazione	ORDINARIO
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	Analisi del fenomeno infortunistico e delle malattie professionali quali: - Raccolta informazioni sugli episodi di infortunio sul lavoro - Assistenza e collaborazione con il Medico Competente nei casi di malattia professionale - Gestione near misses - Adempimenti relativi ai Corsi di Formazione in materia di salute e sicurezza sui luoghi di lavoro, ai sensi dell'at. 36 e 37 del T.U. 81/08 e - Accordo Stato Regioni del 21/12/2011, accreditati ECM. Progettazione, Pianificazione, Gestione e rapporti con l'Unità Operativa -Formazione - Adempimenti relativi ai Corsi di Formazione in materia di antincendio secondo il D.M. 19 marzo 2015 a favore dei dipendenti. - Gestione del personale - Consulenza e pareri per la sicurezza alle varie strutture aziendali - Collaborazione con la direzione strategica per tutte le questioni riguardanti l'applicazione delle misure per la protezione della salute e per la sicurezza dei lavoratori in azienda Rappresentanza del Datore di Lavoro nei riguardi degli Organi di Vigilanza in occasione di verifiche e controlli, in tema di salute e sicurezza nei luoghi di lavori, nelle numerose ASL/AUSL Ospedaliere e	ORDINARIO

		Territoriali dell'Azienda.	
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	TUTELA DELLA SALUTE E DELLA SICUREZZA DEGLI AMBIENTI APERTI E CONFINATI	Attività volte a garantire un livello adeguato di prestazioni in campo ambientale su tutto il territorio, per soddisfare le esigenze di protezione della salute e tutela dell'ambiente previsti dalla Costituzione.	ORDINARIO
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	SORVEGLIANZA E PREVENZIONE DELLE MALATTIE CRONICHE, INCLUSI LA PROMOZIONE DI STILI DI VITA SANI ED I PROGRAMMI ORGANIZZATI DI SCREENING; SORVEGLIANZA E PREVENZIONE NUTRIZIONALE	Tutte le attività di Prevenzione previste dai LEA in aggiunto a quanto previsto dal Prevenzione collettiva e di Sanità Pubblica: screening oncologici e screening neonatali	CRITICO
PREVENZIONE COLLETTIVA E SANITÀ PUBBLICA	SALUTE ANIMALE E IGIENE URBANA VETERINARIA	Tutte le attività che riguardano la Sanità animale, l'Igiene della produzione, trasformazione, commercializzazione, conservazione e trasporto degli alimenti di origine animale e loro derivati e l'Igiene degli allevamenti e delle produzioni zootecniche	ORDINARIO
RETI DI PATOLOGIA	RETI DI PATOLOGIA	reti per patologia che integrano l'attività ospedaliera per acuti e post acuti con l'attività territoriale (es. rete tempo dipendenti)	CRITICO
RISCHIO CLINICO	RISCHIO CLINICO	Sistema di analisi proattivo che tiene in considerazione tutti gli aspetti che possono influenzare la possibilità che un paziente subisca un	CRITICO

		"danno o disagio involontario, imputabile, alle cure sanitarie, che causa un prolungamento del periodo di degenza, un peggioramento delle condizioni di salute o la morte".	
SERVIZI DI FUNZIONAMENTO	ACQUISTI	Gestione dei servizi di supporto agli Acquisti, quali ad esempio: - Gestione di tutti i servizi connessi ai processi di acquisto e approvvigionamento della pubblica amministrazione a partire dalla programmazione del fabbisogno, alla gestione delle diverse procedure di acquisto, fino alla definizione ed all'esecuzione del contratto - Gestione dei servizi connessi alla fase di Pre-Aggiudicazione e Post – Aggiudicazione: gestione dei procedimenti di gara, pubblicazione dei bandi di gara, gestione dei documenti di gara - Gestione delle Gare Telematiche - Gestione della Fattura Elettronica - Gestione dell'Albo Fornitori - Gestione del ciclo di vita dei contratti Gestione di altri servizi legati ai procedimenti di acquisto	ORDINARIO
SERVIZI DI FUNZIONAMENTO	CONTABILITÀ, BILANCIO E CONTROLLO	Gestione dei servizi di supporto alla contabilità e bilancio, quali ad esempio: - Gestione della contabilità finanziaria e fiscale, economico-patrimoniale e della contabilità analitica - Gestione di inventario e patrimonio e dei servizi di economato, di mutui e investimenti, dei servizi di tesoreria - Predisposizione del bilancio di previsione, del rendiconto della gestione degli enti pubblici (comprensivo di stato patrimoniale e conto economico) e del bilancio consolidato - Supporto delle attività di monitoraggio e controllo dei costi e dell'utilizzo delle risorse assegnate - Supporto attività di controllo delle partecipate dell'ente - Supporto attività degli organi istituzionali	ORDINARIO

		dell'ente (nomine, cessazioni, atti, sedute, interrogazioni, ecc.), nonché dei rappresentanti dell'ente presso altri enti, aziende ed istituzioni. Atti deliberativi. – Gestione di altri servizi legati alla contabilità, bilancio e controllo di gestione Supporto attività burocratiche e legali	
SERVIZI DI FUNZIONAMENTO	GESTIONE DOCUMENTALE	Gestione delle operazioni di acquisizione, classificazione ed archiviazione di documenti elettronici, eventualmente firmati digitalmente. Dematerializzazione dei documenti, per la loro gestione e condivisione digitale Definizione di workflow di approvazione	ORDINARIO
SERVIZI DI FUNZIONAMENTO	PERSONALE	Gestione dei servizi di supporto al personale e all'organizzazione, quali ad esempio: - Gestione giuridica e amministrativa di tutti i servizi connessi al personale quali: rilevamento presenze e assenze, gestione fiscale, paghe e contributi della forza lavoro, gestione cedolini, gestione dei piani di sviluppo professionale e di formazione (compresa l'erogazione di formazione e-learning), gestione del processo di performance management dei dipendenti, pianificazione del fabbisogno di personale e recruiting. - Gestione della forza lavoro (workforce management) quali: gestione e pianificazione delle attività di operatori tecnici sul campo, ecc. - Gestione di altri servizi legati al Personale e all'Organizzazione	ORDINARIO
SERVIZI DI FUNZIONAMENTO	PRODUTTIVITÀ INDIVIDUALE E COLLABORATION	Gestione della Produttività individuale e Collaboration, ovvero servizi di Posta Elettronica ordinaria e certificata, Instant Messaging, Social Collaboration Aziendale, creazione, modifica, condivisione dei documenti, presentazioni, fogli di calcolo, ecc.	ORDINARIO
SERVIZI DI	PROTOCOLLO	Gestione delle operazioni di generazione,	ORDINARIO

FUNZIONAMENTO		assegnazione e registrazione di un protocollo informatico ai documenti gestiti dalla pubblica amministrazione Digitalizzazione del registro di protocollo informatico	
SERVIZI INFORMATIVI	COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	Gestione comunicazioni istituzionali web, open data e social.	ORDINARIO
SERVIZI INFORMATIVI	RAPPORTI CON L'UTENZA - URP	Ufficio Relazioni con il Pubblico (URP) dedicato alla semplificazione dei rapporti tra cittadino ed Amministrazione. Offre sia servizi di sportello, per il contatto diretto e per l'accesso ai servizi telematici, sia strumenti di informazione e autoconsultazione, in attuazione della semplificazione di accesso alle informazioni ed ai servizi comunali.	ORDINARIO

Si specifica che dei 40 servizi sopra indicati, i servizi di ASSISTENZA DISTRETTUALE – ASSISTENZA RESIDENZIALE E SEMI-RESIDENZIALE, ASSISTENZA DISTRETTUALE – CURE DOMICILIARI (ANCHE PALLIATIVE), ASSISTENZA DISTRETTUALE – EMERGENZA SANITARIA TERRITORIALE, ASSISTENZA OSPEDALIERA – ATTIVITÀ TRASFUSIONALI sono di ownership regionale e il relativo Fabbisogno relativo viene riportato all'interno del documento centralizzato predisposto da Regione Lazio.

Al fine di completare il quadro descrittivo dell'attuale configurazione adottata dall'Amministrazione, si riporta di seguito la descrizione schematica delle risorse ad oggi impiegata per l'erogazione dei servizi oggetto di migrazione.

AMBITO	VALORE	DOC DI DETTAGLIO
Numero di Data Center e dislocazione sul territorio nazionale	3	
Presenza del servizio di Business Continuity	No	
Presenza del servizio di Disaster Recovery	No	

Polo Strategico Nazionale

Quantità e tipologia di sistemi server (divisione tra sistemi fisici e sistemi dedicati alla farm virtuale)	Circa 600 (200 fisici, 400 virtuali)	
Quantità e tipologia di Storage (SAN, NAS) (con TB presenti, occupati e disponibili)	- SSP NAS netgear 4312 (#3); - Infortrend 3024R2 (#1); – SFN infortrend 3024R2 (#1); – NOM Qnap TS879RP01 (#3)	
Apparati SAN (quantità e caratteristiche della fabric)	No	
Rete (quantità e caratteristiche: Bilanciatori, piano di indirizzamento, eventuali problemi nel cambio di indirizzamento IP)	FW Fortinet & HA Proxy	
Sistemi di sicurezza (quantità e caratteristiche) (Identity & Access Management, Firewall, Sonde, Waf, Soc, etc.)	PAM, Firewall, Sonde, WAF, SOC, EDR,VPN	
Servizio di Active Directory	SI, Windows 2016	
Sistemi di virtualizzazione (VMware, Hyper-V, RedHat)	VMware	
In caso di presenza di VMWARE specificare: N° di vCenter e versioni	3	6.0 – 6.5 -6.7
In caso di presenza di VMWARE specificare: Presenza di prodotti NSX-T, vRNI, vROPS, HCX, etc.	No	
Sistemi fisici dedicati alla farm Vmware	16	
Storage fisici dedicati alla farm Vmware	NOM (2 vol DELL + Qnap); – SSP HPE (#4)	
Presenza di sistemi Iperconvergenti (vSAN, nutanix, DELL VxRAIL, tec.)	SI Nutanix 20220304.342	
Backup, prodotti utilizzati (N° master e N° media server)	Veeam 2 nodi	

Policy di Backup (TB sottoposti a backup e retention)	300 TB	
Librerie e storage dedicati al backup	SI	FUJITSU LT40 LTO6
Piattaforme middleware (quantità e caratteristiche), identificare applicazioni single istance	N.D.	
Identificazione cluster di sistema operativo (Windows, RedHat, Solaris, etc.)	Windows, Oracle	
Database (quantità e caratteristiche)	Oracle + MS SQL	
Sistemi di posta elettronica (PEL e PEC)	Zimbra + Microsoft Exchange	
Siti e portali (quantità e caratteristiche)	10	
È presente una stima del capacity? (eventuale previsione di crescita) in caso affermativo fornire i dati	No	
Presenza di un CMDB accurato del cliente con elenco delle applicazioni	Portale interno Archivio	
Il Data Center sorgente è gestito internamente o da fornitori terze parti?	Terze parti (AQ System Management)	
Le applicazioni vengono gestite internamente o da fornitori terze parti?	Terze parti (AQ System Management et al.)	
Sono disponibili strumenti di monitoraggio delle applicazioni e della rete?	PRTG	
Presenza e tipologia di appliance fisiche	Sonde	
Prodotti Antivirus	Sophos	
Sistema di gestione delle password	Portale interno Archivio	
Qual è il numero totale di workloads presi in considerazione per questo progetto?		
Eventuali workload fisici da migrare (tipologia e quantità) (P2V)		

Tipologie e versioni di sistema operativo (Windows, Linux, etc.)	Windows 2003,2008, 2012, 2016, 2019, RHEL 7.0, RHEL 5, RHEL 8, CentOS 7, Ubuntu 20, Ubuntu 22	
Contesto applicativo – numero di applicativi	Circa 100	

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Titolo	Documenti consegnati	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"

Riferimento	Codice	Titolo
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
AI	Artificial Intelligence
CaaS	Container as a Service
CMP	Cloud Management Platform
CRC	Cyclic Redundancy Check
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
ETL	Extract Transform and Load
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
SCORM	Shareable Content Object Reference Model
VM	Virtual Machine
WBT	Web Based Training
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

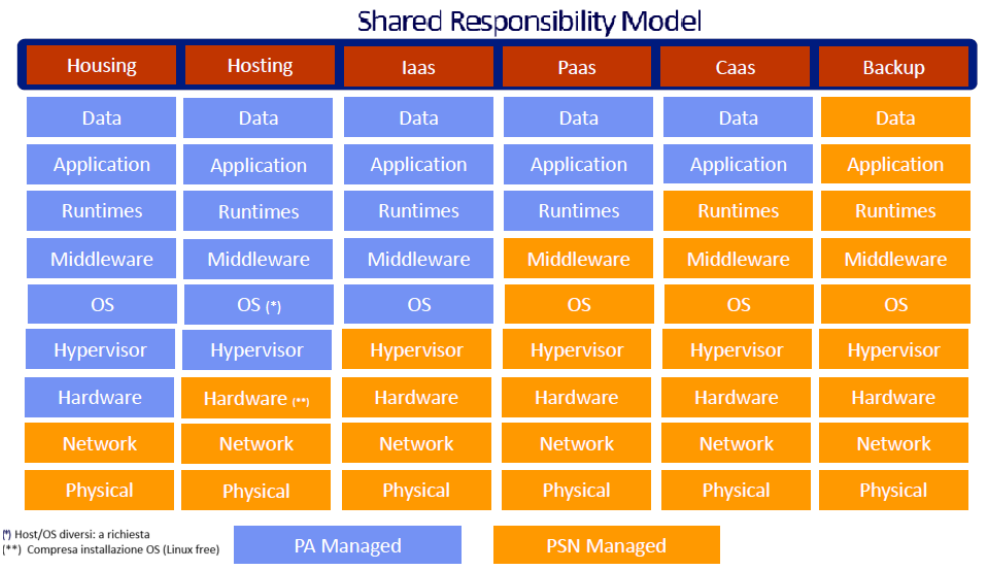
Di seguito si riporta una sintesi delle soluzioni individuate per soddisfare le esigenze dell'Amministrazione.

Servizio	Tipologia
Public Cloud PSN Managed	
Secure Public Cloud	
Servizi di Migrazione	
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

Tabella 9: Servizi Proposti

Le parti concordano di stabilire un coordinamento continuativo e sistematico rispetto alla gestione condivisa della sicurezza dei servizi Cloud acquistati nell'ambito della convenzione, nei limiti e nei ruoli definiti nella matrice di responsabilità.
Le parti si impegnano a informare tempestivamente (in accordo con le normative specifiche di settore) la controparte riguardo l'occorrenza di eventuali incidenti di sicurezza nei propri ambiti di competenza, rispetto alle aree di responsabilità individuate in "matrice di responsabilità" del servizio, nonché a eventuale ulteriore documentazione contrattuale integrativa.
Le comunicazioni dalla P.A. cliente verso PSN dovranno avvenire attraverso i canali previsti per la clientela, ovvero attraverso ulteriori canali comunicati da PSN.

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

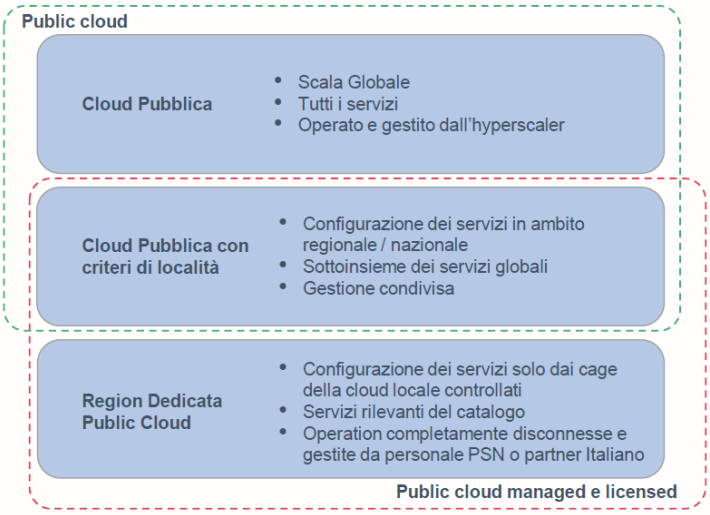


Di seguito, è mostrato il link per consultare la matrice di responsabilità nell'ambito della gestione dei servizi migrati su PSN:
https://www.polostrategiconazionale.it/chi-siamo/sicurezza/matrici-di-responsabilita-condivisa-della-sicurezza/

5.1.1 Descrizione del servizio

Il Public Cloud PSN Managed è un servizio PSN Core che permette alle PA di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica degli ambienti e gestione operata da personale PSN.
Relativamente al modello di servizio Public Cloud PSN Managed, nella prima figura che segue vengono messe in risalto le differenze e integrazioni con il modello Public Cloud puro in Region Italiana; nella seconda se ne descrivono l'architettura e l'interconnessione.

Polo Strategico Nazionale



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

Figura 1 Public Cloud vs Public Cloud Managed

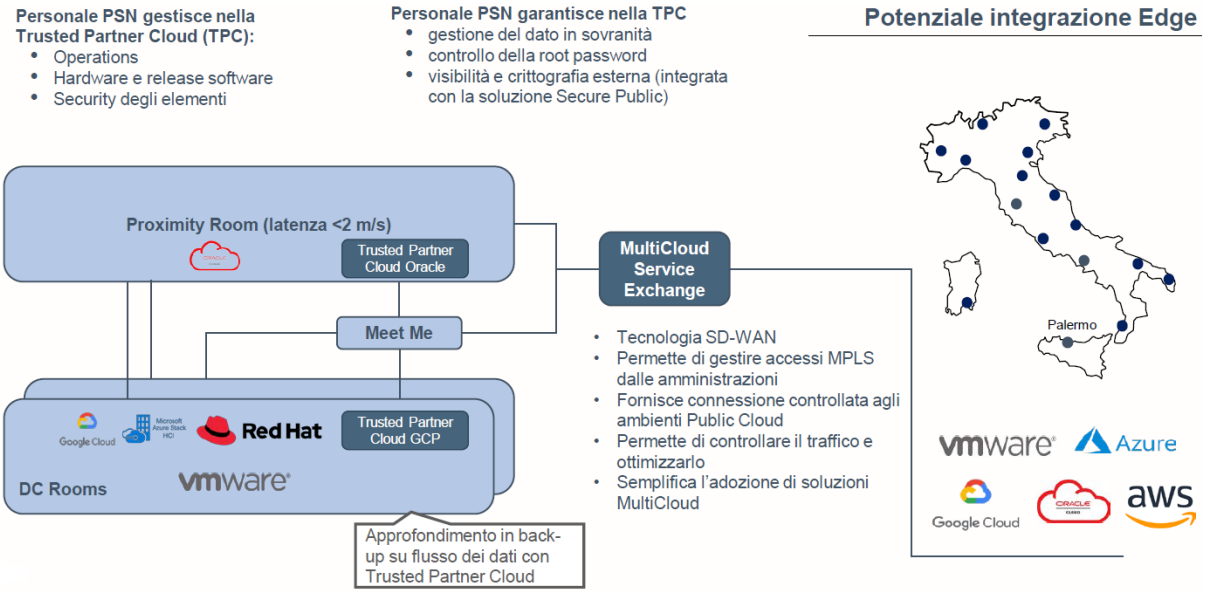


Figura 2 Architettura Public Cloud Managed

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

GCP (Google Cloud Platform)

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

- Segregazione Sicurezza di Rete;

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

Oracle Cloud

Per quanto concerne Oracle, la soluzione nativa è realizzata sul modello di Oracle Region Dedicated. L'architettura prevede una modularità in grado di sfruttare sia singoli componenti tecnologici dedicati (es. x86 systems, Exadata appliance, ecc), sia l'intera Region, in contiguità con la Region Google.
La gestione di tali servizi include in particolare le seguenti aree di attività:

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

Il servizio

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

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

Il PSN dispone di istanze del cloud Hyperscaler aggiungendo i propri domini, indirizzi IP, branding, fatturazione ed è integrato con servizi di Crittografia del PSN stesso. Queste istanze possono essere totalmente disconnesse nel caso sorga la necessità di tutelare la sicurezza nazionale.
Tale Region dedicata può essere usata per i massimi livelli di confidenzialità dei dati grazie alla sua implementazione dedicata al PSN, garantendo però allo stesso tempo tutti i vantaggi di un cloud Hyperscaler quali ad esempio elasticità, completezza di servizi, innovazione e scalabilità.
Gli attori coinvolti nella realizzazione del servizio Public Cloud PSN Managed sono:

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

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

- Ispezione dei controlli: possibilità di ispezionare l'implementazione e il funzionamento dei controlli del CSP. Ciò include audit del codice, l'accesso alla telemetria di sicurezza e la disponibilità di strumenti per applicare e monitorare l'implementazione dei controlli dei propri clienti sul CSP Public Cloud;
- Approvazione e autorizzazione: alcune classi di accesso amministrativo ai dati, implementazioni di sistemi critici, deploy e modifiche del codice, modifiche operative richiederanno un'esplicita approvazione da parte del PSN per la relativa attuazione;
- Root of Trust esterna: il PSN controlla la root of trust per tutti i dati dei clienti. In caso di comportamento non reputato appropriato da parte del CSP, il partner potrà revocargli l'accesso ai dati comuni.

Architettura fisica
Il Public Cloud PSN Managed è implementato all'interno di una delle Region dedicata al PSN, prevedendo la possibilità di fornire un disaster recovery in un'ulteriore Region collocata fisicamente ad almeno 100Km di distanza dalla principale per garantire resilienza in caso di eventi di disastro.
Nelle zone il CSP individuerà delle aree per isolare fisicamente gli apparati dedicati al PSN, e l'MSP-PSN avrà in carico il totale controllo degli accessi a tali aree (se necessario anche inibendo del tutto l'accesso al CSP). In caso di necessità il personale del CSP potrà accedere (ad esempio per fare degli interventi on-site), ma dovrà essere sempre accompagnato da un responsabile dell'MSP-PSN (accesso escorted).
Sarà possibile per l'MSP-PSN anche ispezionare gli strumenti e le apparecchiature usate per gli interventi.
Ripartizione delle responsabilità
Il modello Public Cloud PSN Managed prevede una ripartizione delle responsabilità che lascia all'MSP-PSN il pieno controllo dei layer che vanno dalla gestione logica della rete fino alla sicurezza applicativa.
Il CSP ha la responsabilità di gestire il provisioning dell'HW e degli altri asset fisici e di fornire la piattaforma software per la gestione e l'implementazione dei servizi, lasciando comunque all'MSP-PSN la possibilità di fare code inspections e la review delle modifiche.
Controllo della Rete
L'MSP-PSN ha piena autonomia e totale controllo del traffico di rete da e verso il PSN. Il controllo prevede la possibilità di ispezionare, loggare e bloccare tutto il traffico, mediante dei control proxy scelti da vendor certificati (e non necessariamente forniti dal CSP). Il controllo del traffico riguarda sia i dati (payload) che il traffico per il controllo e l'amministrazione. Tutto ciò a garanzia della totale copertura del rischio di data extrafiltration e di accessi non autorizzati ai sistemi.
Accesso verso l'esterno Frontend
L'MSP-PSN fornisce, gestisce e controlla tutti gli accessi alla rete pubblica: Blocchi di indirizzi IP, peering con le reti di altri providers, ecc.

Se richiesto l'MSP-PSN potrà disporre anche di propri DNS, load balancer, VIP tunneling e strumenti di gestione aggiuntivi.
Rientra inoltre sotto il controllo dell'MSP-PSN anche tutta la gestione delle key chains: nomi di dominio, certificati TLS, CA, rotazione delle chiavi, scadenza, ecc.
Encryption at-rest
Tutti i dati verranno cifrati in modo trasparente at-rested in-transit. Le chiavi di cifratura saranno custodite dall'MSP-PSN su apparati certificati (HSM) di sua proprietà e collocati fisicamente all'esterno del perimetro controllato dal CSP. L'accesso alle chiavi custodite nell'HSM dell'MSP-PSN sarà sempre soggetto ad approvazione ed audit (sia nel caso di accesso consentito, sia nel caso di accesso negato). L'auditing dovrà avvenire su dei sistemi di persistenza che escludano il rischio di manomissione dei log (sia cancellazione che modifica). Il CSP in nessun modo avrà accesso fisico o disponibilità di utenze con privilegi di accesso all'HSM. Tutti i dati (inclusi i backup) custoditi all'interno del Public Cloud PSN Managed saranno cifrati con questo meccanismo. Sarà cura dell'MSP-PSN custodire le chiavi garantendo l'alta disponibilità e la protezione da eventuali eventi di disastro, per scongiurare l'impossibilità di poter decifrare i dati.
Gestione degli Aggiornamenti
Tutti i CSP prevedono degli aggiornamenti frequenti sia ai servizi che ai sistemi di gestione (Continuos deployment) per rilasciare fix, nuove features o rimedi ad esposizioni di sicurezza: uno dei vantaggi del Public Cloud PSN Managed consiste proprio nel poter sfruttare questi benefici (soprattutto la celerità nel rimediare a potenziali esposizioni di sicurezza). Allo stesso tempo però l'MSP-PSN deve tutelare il PSN da eventuali modifiche che in modo malevolo (anche senza la consapevolezza del CSP) possano mettere a rischio la sicurezza delle applicazioni o dei dati.
Modello di Supporto
Il modello di supporto prevede tre livelli con la seguente assegnazione di responsabilità:

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

5.1.2 Personalizzazione del servizio

Il dimensionamento delle risorse valorizzate nel progetto PSN Managed Oracle si compone di:

- Risorse Computazionali IaaS sulle quale verranno configurate le 270 VM dall'Amministrazione per un totale di 553 oCPU, 3.899 GB di RAM e 138.162 GB di Disco.
- Risorse Computazionali PaaS Oracle per un totale di 80 oCPU in modalità BYOL
- Risorse Object Storage per un totale di 307.200 GB dedicati alla Data-Protection nativa della soluzione di cui 20.480 GB riservati per il backup delle istanze Oracle Database
- Risorse Network Firewall e Web Application Firewall per ogni istanza
- Collegamento interno alla network RANSAN tramite n.2 link a 10GB

Si specifica che nel presente Progetto del Piano dei Fabbisogni è prevista la messa a disposizione dei database Oracle in modalità BYOL (Bring Your License), permettendo all' Amministrazione di riutilizzare le licenze ULA in proprio possesso.

All'avvio del progetto e/o durante la fase di progettazione esecutiva, verranno eventualmente rivisti con il Cliente i servizi sottoscritti e/o eventualmente nuovi disponibili da listino PSN, i quali saranno opportunamente valutati se idonei allo scope e obiettivi del progetto.

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

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

5.1.4 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 SECURE PUBLIC CLOUD

5.2.1 Descrizione del servizio

Il Secure Public Cloud è un servizio PSN Core che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza (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 dai Data Center del PSN distribuiti sul territorio Nazionale, nella quale verranno configurati servizi atti a garantire l'adeguato livello di sicurezza dei servizi erogati sul Public Cloud (Gestione Chiavi e Backup).

Tale scenario prevede la presenza dei seguenti attori:

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

Il Secure Public Cloud è un servizio core del PSN che garantisce alti standard di sicurezza:
GESTIONE DELLE CHIAVI. Relativamente alla gestione delle chiavi la soluzione comprende:

- Impiego di terze parti (e.g., Thales CipherTrust) con grande livello di autonomia nella gestione delle chiavi crittografiche per soluzioni in cloud con il modello Bring Your Own Key (BYOK).
- Soluzione di key management replicata nei due datacenter HA e territorialmente nelle due Region.
- Controllo on-premise per ciascuna fase del ciclo vita delle chiavi, consentendo di eseguire in autonomia:
    - generazione delle chiavi ON-PREMISE tramite l'utilizzo di dispositivi crittografici certificati;
    - esecuzione dei backup delle chiavi;
    - installazione diretta delle chiavi sui Key Vault in cloud;
    - monitoraggio degli accessi alle chiavi;
    - rotazione manuale o periodica delle chiavi;
    - revoca delle chiavi.
- On-Prem HSM certificato FIPS 140-2 L3 con partizioni multiple per la corretta gestione del materiale crittografico (chiavi simmetriche ed asimmetriche, generazione entropia, ..).
- CipherTrust Manager per la gestione del ciclo di vita delle chiavi on-premise e in Cloud.
- CipherTrust Cloud Key Manager come orchestratore dei processi di gestione delle chiavi in Cloud. Generazione delle chiavi on-premise per importazione sicura sul cloud provider per tutto il ciclo di vita.

GOVERNANCE MODEL. Per ogni cliente viene creato un ambiente standard segregato e auto-consistente in cui, tramite servizi di delega dei privilegi (ad esempio Azure Lighthouse e Privileged Identity Management) è possibile proiettare i servizi di monitoraggio e sicurezza dello specifico ambiente cliente verso l'ambiente del gestore del PSN che quindi avrà:

- Visibilità di tutti gli ambienti
- Capacità di intervento automatizzato su larga scala
- Possibilità di enforcement delle policy definite

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

- Gestione uniforme e standardizzata dei tenant cliente;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, di set di regole di sicurezza predefinite in linea con best practices internazionali;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, dei ruoli standard per ogni funzione (Ruoli PSN, Ruoli PA, Ruoli terze parti);
- Disponibilità di template securizzati ed integrati a strumenti di sicurezza;
- Gestione unificata dell'identità;
- Gestione degli eventi di sicurezza;

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

- Ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations.

- Usare tecniche di enforcement basate su componenti tecnologiche piuttosto che su processi organizzativi.
- Fornire trasparenza sulle garanzie, i rischi residui e le mitigazioni che si possono implementare.
- I modelli di attacco contro le applicazioni cloud si basano su tecniche diverse per prendere di mira codice o dati in uso, ad esempio:
    - breakout di hypervisor e container;
    - compromissione del firmware ed altre minacce interne, ognuna delle quali si basa su tecniche diverse per prendere di mira codice o dati in uso.

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

SOLUZIONI HUB & SPOKE. Per quanto riguarda l'ambiente Secure Public Cloud è previsto l'uso di un modello Hub & Spoke per consentire al PSN il controllo del traffico e la gestione delle DMZ per l'ambiente cloud.

Le Amministrazioni potranno creare reti virtuali spoke nei segmenti, dove saranno attive Policy che forzeranno la connessione con Virtual Network Hub e impediranno la creazione di tipologie di risorse controllate centralmente, come, ad esempio, gli indirizzi IP pubblici.

BACK UP. Per esercitare la sovranità del dato, il Secure Public Cloud prevede l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP tramite ulteriore livello di archiviazione.

Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup del PSN in modo che lo Storage su cui risiede il dato protetto sia gestito dal personale PSN.

L'integrazione prevede l'uso di tecniche di backup snapshot o stream-based e la cifratura dei dati "at rest" e in transito per garantire la protezione e il ripristino delle macchine virtuali a cui è rivolto il servizio, anche di quelle che implementano meccanismi di encryption del disco di sistema e dei dischi dati.

5.2.2 Personalizzazione del servizio

In base alle indicazioni dell'Amministrazione e a valle di una analisi delle soluzioni infrastrutturali di perimetro PSN, il progetto prevede di utilizzare la proposta di SPC Azure per i servizi ordinari, che non interagiscono direttamente con DB Oracle, indirizzati in PSN Managed, e i servizi di posta elettronica e collaboration Microsoft.

Di seguito una rappresentazione schematica delle risorse computazionali destinate ai suddetti servizi.

Posta elettronica e collaboration

Tipologia	Elemento	Q.tà	Note
Compute Prodution	c4r16	49	

Managed Disks	dischi SSD Standard (128 GB)	120	
Managed Disks	dischi SSD Premium (128 GB)	22	

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

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

5.2.4 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.

5.3 CONSOLE UNICA

La Fornitura prevede l'erogazione alle PAC/PAL, 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".

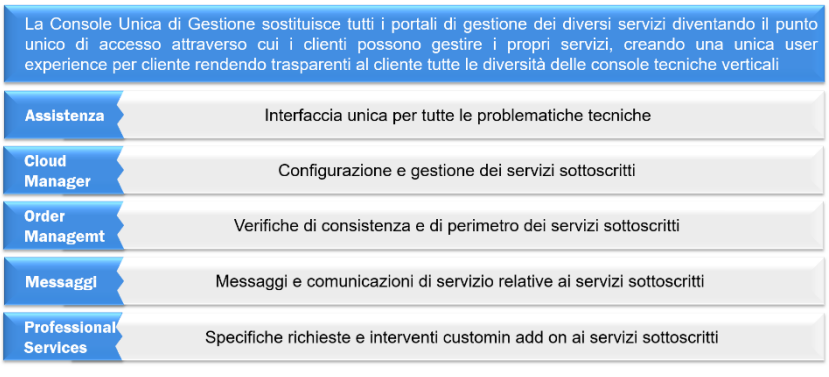


Figura 3 Funzionalità CU

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:
    a. saranno caricati i dati contrattuali ed anagrafici dell'Amministrazione;

b. sarà 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;
c. 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.).

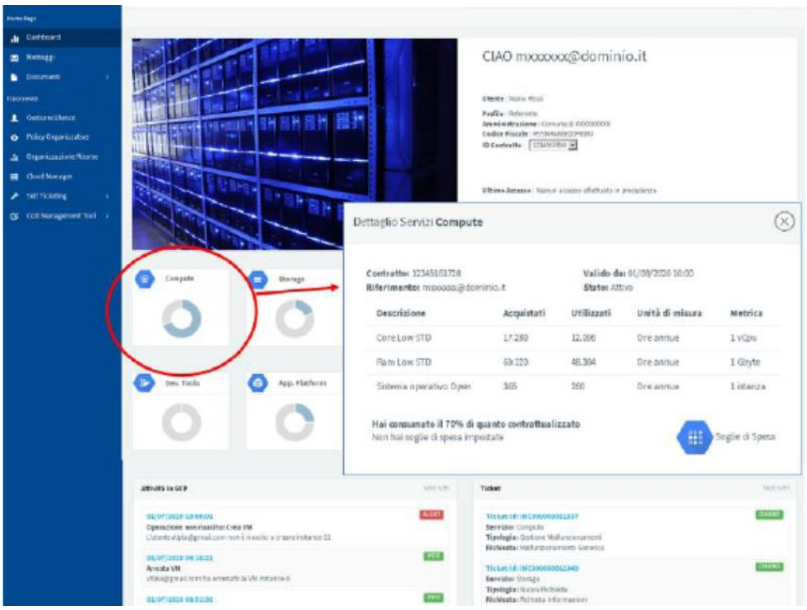


Figura 4 Dashboard CU

- 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.

La migrazione al Polo Strategico Nazionale (PSN) per l'ASL Roma 1 è un'impresa complessa che richiede una visione d'insieme e un approccio olistico. L'infrastruttura IT, con le sue

interdipendenze tra le applicazioni, rappresenta un intricato sistema che non può essere affrontato in modo frammentario.
L'approccio prescelto per la migrazione è basato sulla reinstallazione di macchine virtuali (VM) all'interno del cloud di destinazione. Questa strategia prevede la ricostruzione delle VM esistenti nel nuovo ambiente cloud, mantenendo intatto il codice applicativo e le configurazioni, semplificando così la migrazione stessa. Al fine di assicurare la continuità dei servizi, la fase di installazione dei software prevede l'ingaggio da parte dell'Amministrazione degli enabler applicativi.
L'Amministrazione ha la governance e la responsabilità nella gestione delle fasi di implementazione ed esecuzione di test funzionali e di verifica degli applicativi migrati; il PSN supporterà comunque l'Amministrazione nella conduzione dei suddetti test.

Durante la fase preparatoria della migrazione saranno 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 consiste in un documento di dettaglio che verrà consolidato nella fase di progettazione della migrazione e sarà 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 5: Servizio di Migrazione - Metodologia EMG2C

1. ANALISI/DISCOVERY
   - Analisi piattaforme: Identificare, inventariare, mappare dipendenze e documentare componenti hardware e software da migrare.
   - Analisi applicazioni: Elencare, caratterizzare, analizzare flussi di lavoro e dati, e documentare applicazioni da migrare.
   - Analisi dati: Identificare, classificare, determinare caratteristiche, valutare requisiti di conversione e definire piano di gestione per i dati da migrare.
   - Finestre di migrazione: Individuare periodi a basso impatto, considerare fattori stagionali e risorse, coordinare con manutenzioni e ottenere approvazioni.
   - Indisponibilità applicazioni: Stimare tempi di inattività, comunicare agli utenti, fornire alternative di accesso e definire piani di rollback.
   - Analisi sicurezza: Valutare rischi in ambienti di origine e destinazione, identificare vulnerabilità, implementare controlli di sicurezza e sviluppare un piano di risposta agli incidenti.
   - Piano di migrazione di dettaglio: Definire obiettivi, portata, metodologia, team, risorse, cronogramma, procedure di test e rollback, documentazione completa e comprensibile.

2. SET-UP
- Predisposizione dell'infrastruttura target presso i nuovi DC
  - disegno dei workload;
  - definizione architettura logica e fisica;
  - configurazione ambienti;
  - creazione, gestione e configurazione VM;
  - predisposizione dei middleware di base (Tomcat, Liferay, Kafka ecc) con le relative configurazioni;
  - installazione e configurazione degli eventuali Database IaaS utilizzando le configurazioni on-premise
  - configurazione networking e regole firewall;
  - configurazione sistema di monitoraggio (Prometeus, Nagios e Elk centralizzato);

3. MIGRAZIONE

Il trasferimento dei dati è una parte fondamentale del processo di migrazione verso il cloud. La migrazione dei dati prevede:

- Migrazione dei dati per tutti i database applicativi (Oracle, Postgresql, Mongodb, Mysql, SQL Server, MariaDB);
- Implementazione policy di sicurezza;
- Predisposizione delle configurazioni dei backup in base alle politiche definite nel Piano di Migrazione di Dettaglio

4. MIGRAZIONE su Secure Public Cloud

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;
- Valutazione dei requisiti: analisi di fattibilità della migrazione e valutazione delle possibili issue di compatibilità da risolvere;
- Progettazione architettura cloud: progettazione della best-solution per concretizzare le necessità del cliente con le soluzioni disponibili like PSN;
- Cloud Assesment: valutazione dei rischi legati a garantire la sicurezza, la riservatezza e la disponibilità dei dati;
- Target Design: condivisione delle soluzioni che verranno messe in atto e dell’architettura scelta per soddisfare le esigenze del cliente;
- Target Build: realizzazione e messa in attività delle risorse al fine di predisporre l’ambiente ad effettuare la migrazione (Secure Landing Zone);
- Pianificazione migrazione: redazione del runbook e della documentazione per definire la strategia di porting dei workload;
- Migration Execution: esecuzione di tutti gli step di migrazione dalla copia dei dati alla messa in produzione degli stessi;
- Verifica e Testing: verifica del corretto funzionamento e della corretta erogazione dei servizi, redazione del documento di hand-over.

Secure Public Cloud Azure - Migrazione L&S

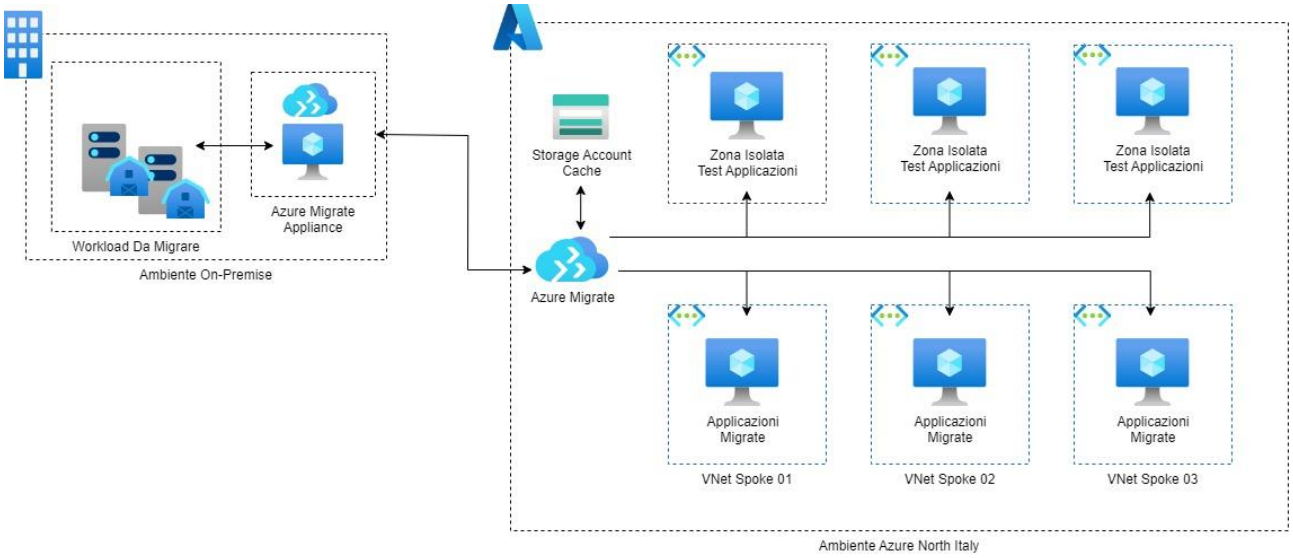


Tabella 10: SPC - Migrazione L&S

Le metodologie di migrazione sono pensate per ridurre al minimo gli impatti sull'erogazione dei vari workload di produzione. Ogni singolo sistema verrà migrato tenendo conto delle best practices Microsoft Azure, quindi:

- L'allineamento dei dati avverrà senza rallentare il throughput della componente storage di produzione;
- I workload durante la fase di test e validazione verranno accesi in una bolla isolata per non creare problematiche network con la produzione;
- Le applicazioni e i servizi a bordo delle VM non subiranno nessuna modifica al netto delle configurazioni lato cloud, ad esempio network e/o agent Azure, poiché la VM verrà copiata mediante un V2V;
- Instaurando un flusso di replica costante tra le VM On-Prem ed Azure, non ci sarà possibilità di perdita di dati e/o dati non allineati.

Vantaggi Migrazione su Secure Public Cloud:

- Ottimizzazione dei costi.
- Flessibilità e scalabilità dei workload.
- Delivery rapido di workload.
- Governance semplificata e centralizzata.
- Gestione semplificata della componente Backup /BC.

Connettività Datacenter PSN:

- Gestione delle chiavi di sicurezza.
- Sovranità del dato garantito anche per il backup effettuato sui DC del PSN.

- Collegamento dedicato verso i DC del PSN.
- Controllo dei flussi di rete con le tecnologie presenti nell'HUB (FW, WAF).

5. 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.

Di seguito si riporta la tabella del team mix dedicato all'erogazione complessiva del progetto di migrazione e le relative gg/uu.

Profilo Professionale	Q.tà
Enterprise Architect	399
Cloud Application Architect	467
Cloud Application Specialist	1.181
Cloud Security Specialist	1.162
Database Specialist and Administrator	1.162
System Integrator & Testing Specialist	2.563
Project Manager	758
System and Network Administrator	15
Totale	**7.707**

Le quantità rappresentate nella precedente tabella costituiscono per intero l'effort previsto per il completamento del progetto di migrazione. Nei successivi paragrafi verranno rappresentate, nel dettaglio, le quote previste per i principali task di migrazione.

5.4.1 Migrazione DB Oracle

Per quanto inerente i sistemi Oracle, è prevista la migrazione di 15 database così distribuiti:

- 5 nella versione 11.2
- 10 nella versione 19c

Nel rispetto dei requisiti del PSN, i 5 database 11.2 dovranno essere preventivamente innalzati di release alla versione 19c: per questi database si provvederà prima ad un adeguamento dalla versione corrente alla versione 19x e poi il trasferimento verso il PSN. Nel caso di release 11.2.0.4 o successive è possibile eseguire l'aggiornamento diretto come indicato dalla documentazione del fornitore: https://docs.oracle.com/en/database/oracle/oracledatabase/ 19/upgrd/oracle-

Polo Strategico Nazionale

database-releases- that-support-direct-upgrade.html. Nel caso di Database Maintenance release number, 2, o Component specific release number, 4, inferiori al minimo richiesto si applicheranno le patch di prodotto per raggiungere la release necessaria al direct upgrade.

Di seguito si riportano i database con le relative risorse computazionali.

ID	Nome Database	vCPU	RAM GB	Storage GB	Backup storage GB	DB version (**)	Test
1	reapr	8	32	3000	2000	19c	y
2	renoelab	24	128	2500	500	11.2	n
3	revac	32	128	1000	300	11.2	n
4	resfntf	0(*)	0	30	10	11.2	n
5	resfnj	0	0	30	10	11.2	n
6	resfsnc4h	12	128	1000	800	19c	y
7	amlet	8	32	350	200	11.2	n
8	reccrd	8	64	30	15	19c	y
9	gpitrmprd	4	16	30	10	19c	y
10	db1	16	64	100	30	19c	n
11	db2	0	0	100	30	19c	n
12	db3	0	0	100	30	19c	n
13	dms	8	64	400	10	19c	n
14	elipseprod	16	64	2000	500	19c	n
15	areas	16	64	700	400	19c	n

Come descritto in precedenza, la modalità di migrazione utilizzata, ricalcherà la matrice di seguito riportata rispetto all'ambiente target scelto dall'Amministrazione:

Ambiente Target	Backup\Restore	Data Guard
PSN Managed Oracle	**X**	**X**
Industry Standard PaaS DB Oracle	**X**	

Nella tabella, oltre la fase iniziale di predisposizione e di trasferimento iniziale, sono descritte le attività di due differenti modalità di migrazione dei dati che tengono in considerazione l'applicazione e la sua finestra di indisponibilità.

INSERIRE TABELLA DESCRIZIONE WBS

WBS	Task	Descrizione
1	Infrastruttura Cloud DB	Il task racchiude le attività necessarie alla configurazione dell'istanza database
1.1	Predisposizione Istanza Oracle	Creazione dell'istanza e configurazione iniziale riportando quanto presente On Premise
1.2	Security List & Network Security Group	Configurazione delle regole di sicurezza a protezione dell'istanza
1.3	Verifica connettività	Test di raggiungibilità dell'istanza dalle subnet autorizzate e dalle componenti applicative

2	Trasferimento iniziale	Full back dell'instanza on premise, trasferimento verso il Cloud e restore dei dati all'interno dell'istanza target. In questa fase saranno calcolati i tempi end2end di disponibilità del dato.
3	Scenario 1	Scenario in cui la finestra di indisponibilità è tale da non essere compatibile con i tempi rilevati in 2)
3.1	Setup Data Guard	Predisposizione dello strumento di allineamento realtime dei dati
3.2	Test Funzionali & Performance Test	Finestra disponibile al fornitore applicativo per eseguire i test funzionali ed eventuali performance test. In questo task è disponibile il supporto continuativo per il tuning dell'istanza
3.3	Trasferimento per go live	A valle dei test viene clonato nuovamente il database per la conclusione della migrazione
3.4	Attivazione Data Guard	Attivazione della replica realtime dei dati
3.5	Realtime Update	Finestra per l'aggiornamneto del delta dei dati tra il momento del backup on prem ed il restore sul PSN
3.6	Switch	Switch dell'applicazione, smoke test ed attivazione politiche di backup.
3.7	Go Live	Chiusura del processo di migrazione con l'attivazione dell'applicazione sul PSN
4	Scenario 2	Scenario in cui la finestra di disponibilità è tale da essere compatibile con i tempi rilevati in 2)
4.1	Test Funzionali & Performance Test	Finestra disponibile al fornitore applicativo per eseguire i test funzionali ed eventuali performance test. In questo task è disponibile il supporto continuativo per il tuning dell'istanza
4.2	Trasferimento per go live	A valle dei test viene clonato nuovamente il database per la conclusione della migrazione
4.3	Switch	Switch dell'applicazione, smoke test ed attivazione politiche di backup
4.4	Go Live	Chiusura del processo di migrazione con l'attivazione dell'applicazione sul PSN

Di seguito si riporta la tabella del team mix dedicato all'erogazione del servizio e le relative gg/uu.

Profilo Professionale	Q.tà

Enterprise Architect	59
Cloud Application Architect	63
Cloud Application Specialist	175
Cloud Security Specialist	172
Database Specialist and Administrator	172
System Integrator & Testing Specialist	380
Project Manager	99
Totale	**1.120**

5.4.2 Migrazione componenti applicative

Il portafoglio di servizi dell'Amministrazione indicati nel capitolo 2 vengono erogati attraverso un corposo sistema di componenti applicative.

Di seguito si riporta la tabella del team mix dedicato all'erogazione del servizio e le relative gg/uu.

Profilo Professionale	Q.tà
Enterprise Architect	324
Cloud Application Architect	347
Cloud Application Specialist	960
Cloud Security Specialist	945
Database Specialist and Administrator	945
System Integrator & Testing Specialist	2.083
Project Manager	543
Totale	**6.147**

5.4.3 Integrazione ambienti cloud PSN SPC Azure e PSN Managed al Servizio SOC di ASL Roma 1

La migrazione al PSN (Polo Strategico Nazionale) rappresenta un cambiamento significativo per l'infrastruttura IT dell'ASL Roma 1. La gestione post-migrazione prevede integrazione nei servizi SOC e NOC già erogati on-premise. Per garantire una migrazione sicura e efficiente verso ambienti cloud SPC Azure e PSN Managed, il PSN propone un piano progettuale che si articola in diverse fasi:

Fase 1: Analisi e pianificazione

- Valutazione dell'infrastruttura esistente: Identificazione degli asset IT, dei rischi e dei requisiti di sicurezza specifici per la migrazione al PSN.
- Definizione dell'architettura di sicurezza cloud: Progettazione della segmentazione della rete, dei controlli di accesso, delle policy di sicurezza e delle procedure operative specifiche.
- Pianificazione dettagliata del progetto: Definizione di fasi, attività, tempi, risorse e budget per la migrazione al PSN.

Fase 2: Implementazione

- Implementazione delle connessioni di rete sicure tra cloud e on-premise
- Test di connettività e sicurezza: Verifica del corretto funzionamento delle connessioni e dell'efficacia delle misure di sicurezza implementate.

Fase 3: Configurazione e ottimizzazione

- Configurazione delle sorgenti di dati: Impostazione di API, syslog e agent per garantire il flusso corretto dei log e degli eventi di sicurezza.
- Definizione delle policy e delle regole di allarme: Stabilire criteri per la rilevazione e la gestione di minacce e anomalie.
- Formazione del personale: Fornire al personale IT le competenze necessarie per gestire la sicurezza nell'ambiente cloud PSN.

Fase 4: Test e validazione

- Testing completo del sistema di sicurezza: Valutazione approfondita del sistema per identificare e risolvere eventuali vulnerabilità o problemi di configurazione specifici.
- Risoluzione dei problemi e ottimizzazione: Ottimizzazione delle configurazioni per garantire il massimo livello di sicurezza e prestazioni.

Fase 5: Attivazione e monitoraggio

- Attivazione dei servizi SOC di ASL Roma 1: Avvio dei servizi di Security Operations Center per la gestione continua della sicurezza nell'ambiente ibrido.
- Monitoraggio iniziale e fine-tuning: Monitoraggio attento del sistema per identificare e risolvere eventuali problemi e ottimizzare le configurazioni in base alle esigenze nell'ambiente ibrido.

Tutte le nuove sorgenti di log confluiranno nel servizio SIEM attivo (erogato insieme ai servizi SOC e NOC). La gestione coordinata con i "Cloud Enabler" e il presidio sistemistico del cliente garantirà il controllo di tutti i flussi di dati da e verso i sistemi e servizi (VPN IPsec site-to-site e/o autorizzazioni specifiche per accesso/integrazione tramite API).

Di seguito si riporta la tabella del team mix dedicato all'erogazione del servizio e le relative gg/uu.

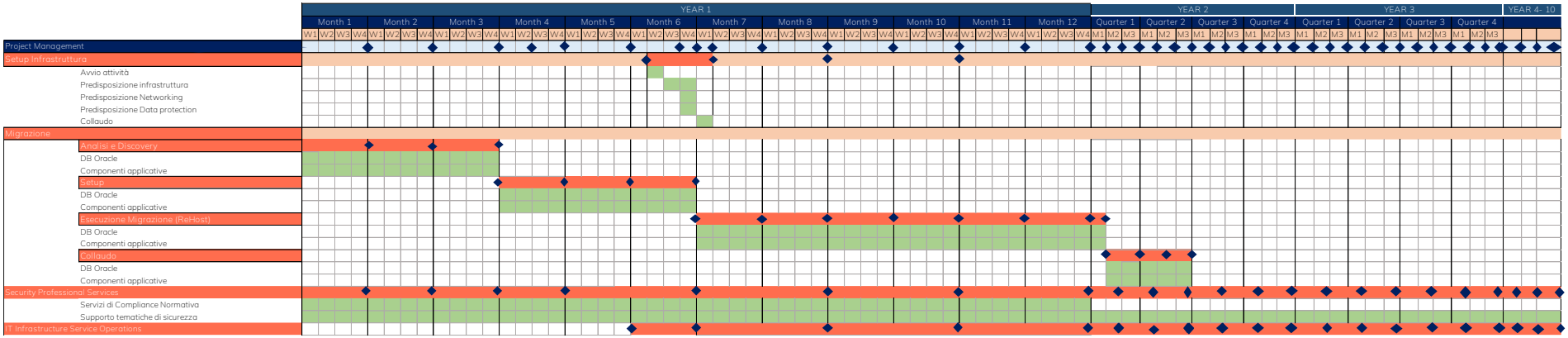
Profilo Professionale	Q.tà

Enterprise Architect	16
Cloud Application Architect	57
Cloud Application Specialist	46
Cloud Security Specialist	45
Database Specialist and Administrator	45
System Integrator & Testing Specialist	100
Project Manager	116
System and Network Administrator	15
Totale	**440**

5.4.4 Piano di attivazione e Gantt

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

Polo Strategico Nazionale



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

Polo Strategico Nazionale

5.4.5 Security Profess. Services

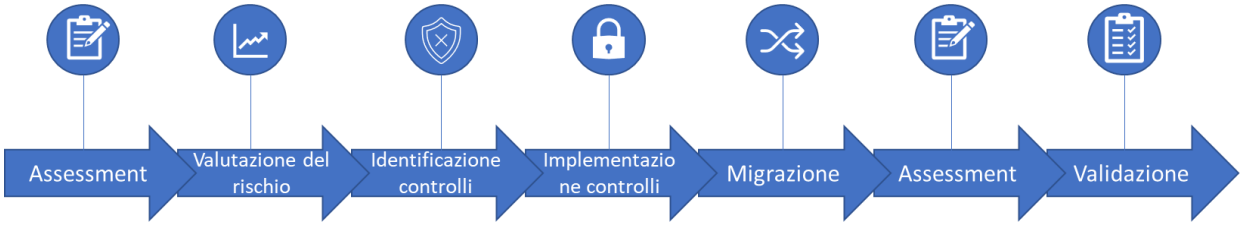
La migrazione su cloud è un processo complesso e un cambiamento rilevante che non va preso alla leggera. Non esiste una procedura di migrazione immediata sul cloud, e anzi spesso i rischi di migrazione stessi non vengono opportunamente valutati con il risultato che un'attività di migrazione che dovrebbe in teoria migliorare il livello complessivo di sicurezza delle applicazioni, di fatto lo diminuisce, esponendo i workload migrati a nuove minacce ed attacchi. È bene specificare che trasferendo le informazioni nel cloud non si trasferisce anche la responsabilità della sicurezza di tali informazioni. Il PSN offre molti strumenti nativi, all'interno delle diverse tipologie di cloud scelte, per gestire la sicurezza dei dati, ma questi devono essere in ogni caso previsti ed implementati dalle Amministrazioni. La responsabilità della sicurezza di tutti i dati trasferiti su cloud rimane sempre e comunque del cliente finale. Il fatto che le infrastrutture cloud siano intrinsecamente dotate di un livello di sicurezza elevato, di per sé non offre alcuna efficace garanzia sulla sicurezza delle informazioni ivi trasferite.

I servizi professionali di sicurezza sono quindi necessari, sinergici e parte integrante dei servizi di migrazione, e servono principalmente a valutare lo stato di sicurezza dei workload da migrare, prima e post migrazione, prevedendo in un approccio security-by-design l'analisi del rischio, l'identificazione, l'implementazione e la gestione dei controlli di sicurezza.

I servizi sono necessari per:

- Garantire la conformità ai requisiti normativi e cogenti.
- Valutare e applicare le best practice di cloud security.
- Mitigare il rischio cyber.
- Valutare rischi e vulnerabilità prima e dopo il processo di migrazione.
- Prevedere, progettare ed implementare i controlli di sicurezza
- Supportare l'Amministrazione nella gestione della cybersicurezza.

Di seguito vengono illustrati i diversi step delle fasi di gestione della sicurezza implementabili tramite i servizi professionali in oggetto



5.4.5.1 Personalizzazione del servizio

Nell'ambito del presente Progetto il PSN ha previsto a beneficio dell'Amministrazione un servizio di consulenza su tematiche verticali riguardanti la sicurezza, al fine di garantire un supporto decisionale ed operativo nel perimetro della cyber security.

Supporto Security										
Profilo Professionale	Anno 1	Anno 2	Anno 3	Anno 4	Anno 5	Anno 6	Anno 7	Anno 8	Anno 9	Anno 10
Project Manager	7	8	8	8	8	8	8	8	8	8
Security Principal	4	5	5	5	5	5	5	5	5	5
Senior Information Security Consultant	5	6	6	6	6	6	6	6	6	6
Junior Information Security Consultant	11	13	13	13	13	13	13	13	13	13
Cloud Application Architect	5	6	6	6	6	6	6	6	6	6
Cloud Application Specialist	11	12	12	12	12	12	12	12	12	12
Security Solution Architect	10	12	12	12	12	12	12	12	12	12
Senior Security Auditor/Analyst	21	24	24	24	24	24	24	24	24	24
Junior Security Analyst	15	17	17	17	17	17	17	17	17	17
Senior Penetration Tester	5	5	5	5	5	5	5	5	5	5
Junior Penetration Tester	10	11	11	11	11	11	11	11	11	11
Data Protection Specialist	13	15	15	15	15	15	15	15	15	15

La responsabilità della configurazione, gestione e manutenzione di misure adeguate alla sicurezza rimane a carico dell'Amministrazione come espresso nel relativo Paragrafo (§ 7-SICUREZZA).
Inoltre di seguito viene descritto un ulteriore consulenza specialistica sulla compliance normativa prevista nelle fasi iniziali del Progetto.

Servizi di Compliance Normativa

I servizi di Compliance Normativa prevedono l'analisi da parte di un team di specialistico di processi, procedure e template documentali al fine di accertare la loro aderenza alle normative vigenti. Il servizio prevede la valutazione delle seguenti tematiche:

COMPLIANCE PRIVACY E FOLLOW-UP: Il servizio ha l'obiettivo di valutare ex ante il gap che separa l'Amministrazione dalla conformità alla normativa di settore europea e nazionale, con specifico riferimento alla predisposizione della documentazione necessaria per l'Organigramma privacy, il Registro dei trattamenti ex art. 30 GDPR, il DPIA ex art. 35 GDPR e le policy privacy aziendali.

SUPPLY CHAIN AUDITING: Il servizio comprende l'erogazione di questionari, audit on-site e da remoto, destinati ai fornitori di riferimento dell'Amministrazione per il censimento e la valutazione delle misure di sicurezza tecniche e/o organizzative adottate nell'ambito delle attività concernenti il trattamento dei dati personali dell'Amministrazione stessa.

CRISIS COORDINATION & DATA BREACH MANAGEMENT: Il servizio prevede la consulenza e il supporto nella gestione di un data breach complesso e impattante sui sistemi informatici aziendali. Nello stesso ambito viene anche prevista l'attività di coordinamento tra la Governance aziendale, il team cybersecurity interno, l'Ufficio Privacy e ogni altra figura professionale

dell'Amministrazione, incardinata nel procedimento. In caso di avvenuto data breach il team impegnato nel task avrà il compito di coadiuvare l'Amministrazione nell'espletamento delle attività di notificazione obbligatorie ed eventuali alle Autorità competenti di settore, oltre che l'attività di comunicazione all'interessato nei casi previsti dall'art. 34 GDPR.

ADVISORING: Il servizio prevede il rilascio di materiale e contenuti informativi su tematiche relative alle politiche adottate in tema di data protection, misure di sicurezza e norme volontarie.

DIRETTIVA NIS 2: Il servizio prevede una serie di attività che hanno l'obiettivo di supportare e assistere l'Amministrazione nella valutazione del proprio livello di conformità e nel conseguente adeguamento alle misure di cybersicurezza di cui alla c.d. Direttiva NIS 2.

Di seguito si riporta la tabella del team mix previsto per l'erogazione dei servizi di sicurezza descritti e le relative gg/uu.

Profilo Professionale	Q.tà
Security Principal	19
Senior Information Security Consultant	23
Junior Information Security Consultant	52
Cloud Application Architect	25
Cloud Application Specialist	50
Security Solution Architect	46
Senior Security Auditor/Analyst	96
Junior Security Analyst	69
Senior Penetration Tester	21
Junior Penetration Tester	45
Data Protection Specialist	58
Project Manager	31
Totale	**535**

5.4.6 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.

Di seguito si riporta la tabella con una vista sulle relative gg/uu previste per singolo anno.

IT Operation										
Profilo Professionale	Anno 1	Anno 2	Anno 3	Anno 4	Anno 5	Anno 6	Anno 7	Anno 8	Anno 9	Anno 10
Systems Architect	0	156	168	168	168	168	168	168	168	168
Product/Network/Technical Specialist	0	1203	1294	1294	1294	1294	1294	1294	1294	1294
Database Specialist and Administrator	0	202	217	217	217	217	217	217	217	217
Cloud Security Specialist	0	134	145	145	145	145	145	145	145	145
System and Network Administrator	0	565	608	608	608	608	608	608	608	608
Project Manager	0	294	316	316	316	316	316	316	316	316

5.4.6.1 Personalizzazione del servizio

Il servizio di IT Infrastructure Service Operation prevede una finestra di servizio H8x7 per le seguenti attività:

- Incident Management;
- Problem Management;
- Change Management;
- Performance Management;
- Patch Manament;
- Database Management;
- Network Management;
- Event Monitoring;
- Cost Control;
- User Management;
- Data Protection;
- Analisi dei log, segnalazioni d'errore;
- Monitoraggio prestazioni di sistema (dischi, memoria, processi);
- Monitoraggio del database (spazio allocato, prestazioni, ecc.);
- Controllo andamento prestazioni delle transazioni concordate con il Cliente;
- Tuning del sistema concordato con la parte applicativa;
- Amministrazione del sistema operativo attraverso i tool standard, incluse le procedure di startup e shutdown secondo modalità ricevute dalla parte applicativa (ad es. con quale ordine devono essere fermati i servizi configurati);
- Patching del sistema operativo, ovvero installazione e applicazione delle patch oppure hot fix rilasciate dal fornitore del sistema operativo, secondo una procedura e una schedulazione da concordare con il cliente e i gruppi applicativi;
- Verifica dei log del sistema operativo e loro gestione;
- Gestione servizio Microsoft Premier: supporto da parte di Microsoft nel caso di problematiche afferenti all'infrastruttura del CSP (dettagli);
- Gestione backup e restore: gestione sistemistica delle operatività connesse alle funzionalità di backup e restore delle risorse e file system;
- Gestione del tenant Azure: gestione sistemistica delle risorse al fine di mantenere la subscription allineata con gli standard qualitativi prefissati;
- Gestione governance: gestione dei processi di implementazione e sviluppo di risorse e servizi.

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.
- Security Principal: Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
- Senior Information Security Consultant: Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
- 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.
- Senior Security Auditor/Analyst: Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia. Completa i giornali di audit documentando test e risultati dell'audit.

- Security Solution Architect: Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.
- 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.
- Junior Security Analyst: Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
- Forensic Expert: E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.
- Senior Penetration Tester: Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.
- Junior Penetration Tester: Effettua tentativi di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza in accordo con quanto definito le progetto di riferimento.
- 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.
- Educational Designer/Tutoring: Struttura, organizza e schedula i programmi di formazione, ne valuta la qualità attraverso un processo di feedback.

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 (10 anni) dei servizi contenuti nel presente progetto sarà declinata all'interno del contratto di utenza.

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	13664791004
Ragione Sociale	AZIENDA SANITARIA LOCALE ROMA 1
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2024-0000013664791004-PPdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	5.3

RIEPILOGO PREZZI				
SERVIZIO		Totale UT		Totale Canone Annuale
Industry Standard	€	-	€	-
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	85.825,06
Public Cloud PSN Managed			€	747.808,47
Servizi di Migrazione	€	2.123.044,45		
Servizi Professionali	€	8.745.063,68		
TOTALE	€	10.868.108,13	€	833.633,53

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT
SP-07	ServiziMigrazione	FiguraMigrazione	Project Manager	758		€ 281.824,4000
SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	399		€ 165.708,6900
SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	467		€ 180.892,4500
SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	1181		€ 372.428,3500
SP-05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	1162		€ 289.698,2200
SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	1162		€ 289.698,2200
SP-12	ServiziMigrazione	FiguraMigrazione	System and Network Administrator	15		€ 4.461,6000
SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	2563		€ 538.332,5200
SP-23	ServiziProfessionali	ITInfrastructureServiceOperation	Systems Architect	1500		€ 725.610,0000
SP-24	ServiziProfessionali	ITInfrastructureServiceOperation	Product/Network/Technical Specialist	11555		€ 3.871.156,1000
SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	1938		€ 483.162,7800
SP-05	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Security Specialist	1294		€ 322.607,1400
SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	5429		€ 1.614.801,7600
SP-07	ServiziProfessionali	ITInfrastructureServiceOperation	Project Manager	2822		€ 1.049.219,6000
SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	68		€ 35.395,3600
SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	82		€ 34.749,1400
SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	180		€ 53.539,2000
SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	84		€ 32.537,4000
SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	169		€ 53.294,1500
SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	164		€ 69.498,2800
SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	333		€ 148.571,2800
SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	237		€ 66.893,2500
SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	71		€ 26.397,8000
SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	154		€ 40.141,6400

Polo Strategico Nazionale

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	206		€ 76.590,8000	
SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	110		€ 40.898,0000	
SEC-MS-07	SecurePublicCloudAzure	ComputeProduction	VM "convenzionali"c4r16	49			€ 41.819,2411
SEC-MS-42	SecurePublicCloudAzure	Storage	Managed Disks - dischi SSD Standard (128 GB)	120			€ 12.172,0560
SEC-MS-43	SecurePublicCloudAzure	Storage	Managed Disks - dischi SSD Premium (128 GB)	22			€ 5.036,1256
SEC-MS-47	SecurePublicCloudAzure	Network	Bandwidth Internet - TB annui	3			€ 231,0123
SEC-MS-54	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	2			€ 1.647,4852
SEC-MS-55	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	3			€ 2.368,2912
SEC-MS-56	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	6			€ 751,3614
SEC-MS-57	SecurePublicCloudAzure	PublicCloudSecurityBackupMonitor	Monitor VM Data ingestion - GB per giorno	2			€ 1.578,8608
SEC-MS-59	SecurePublicCloudAzure	PublicCloudSecurityBackupFirewall	Deployment - Istanze	1			€ 13.490,9455
SEC-MS-60	SecurePublicCloudAzure	PublicCloudSecurityBackupFirewall	Data managed - TB mese	1			€ 173,0636
SEC-MS-61	SecurePublicCloudAzure	PublicCloudSecurityBackupCloudBackup	Istanze Protette - Numero VM	24			€ 2.548,6176
SEC-MS-62	SecurePublicCloudAzure	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	16000			€ 4.008,0000
MGD-GCP-001	PublicCloudPSN Managed	LicensedCloudHyperscalerTechnology	vCPUs - General Purpose N2	553			€ 65.794,8340
MGD-GCP-011	PublicCloudPSN Managed	LicensedCloudHyperscalerTechnology	Memory - General Purpose RAM	3899			€ 50.360,2638
MGD-GCP-020	PublicCloudPSN Managed	LicensedCloudPersistentStorageHyperscalerTechnology	Storage - Balanced PD	138162			€ 134.017,1400
MGD-GCP-044	PublicCloudPSN Managed	LicensedCloudStorageHyperscalerTechnology	Cloud Storage - Standard Storage Regional	307200			€ 59.596,8000
MGD-GCP-060	PublicCloudPSN Managed	Networking	Networking Cloud Load Balancing HTTPS External Regional Forwarding Rule Europe	10			€ 836,3740
MGD-GCP-061	PublicCloudPSN Managed	Networking	Networking Cloud Load Balancing HTTPS External Regional Inbound Data Processing Europe	10			€ 573,5790
MGD-OCP-118	PublicCloudPSN Managed	LicensedSQLeOracleHyperscalerTechnology	SQL instances - Gen 2 Exadata Cloud at Customer - Database OCPU - BYOL	80			€ 195.106,2960
MGD-OCP-126	PublicCloudPSN Managed	LicensedSQLeOracleHyperscalerTechnology	SQL instances - Oracle Autonomous Transaction Processing - Exadata Storage	13			€ 193.939,2000
	PublicCloudPSN Managed	Licensed Security Cloud Solution	Cloud Operations -Logging ingestion (free from 0 to 50GB)	6200			€ 35.043,6400
	PublicCloudPSN Managed	Licensed Security Cloud Solution	Cloud Operations -Logging storage (logs retained more than 30 days)	10240			€ 993,2800
	PublicCloudPSN Managed	Licensed Security Cloud Solution	Cloud Operations - Cloud Monitoring (5K metric size, 60 metric x hours)	36			€ 16,9848
MGD-GCP-167	PublicCloudPSN Managed	LicensedSecurityCloudSolution	Cloud Security - Cloud Armor	2			€ 11.530,0826

Polo Strategico Nazionale

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.
La schematizzazione della rendicontazione riportata di seguito rappresenta una proposta non vincolante per le parti.

			Anno 1												Anno 2				Anno 3			
Servizi di Migrazione (Milestone Based)	Peso	Importo	Month 1 - Startup	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		€ TOT																				
- Analisi & Discovery	30%	2.123.044,45 €	20%	65%	15%																	
- Setup	20%					30%	40%	30%														
- Migrazione	45%								10%	15%	15%	25%	15%	15%	5%							
- Collaudo	5%														10%	90%						
Servizi professionali (canone mensile		€ TOT																				
- IT Service Operation	100%	1.742.990,20 €													8,33%	16,67%	8,33%	16,67%	8,33%	16,67%	8,33%	16,67%
- Security Professional Services - Compliance Normativa	100%	194.982,45 €		16,67%		16,67%		16,67%		16,67%		16,67%		16,67%								
- Security Professional Services - Supporto Sicurezza	100%	140.599,24 €		5,56%		5,56%		5,56%		5,56%		5,56%		5,56%	5,56%	11,11%	5,56%	11,11%	5,56%	11,11%	5,56%	11,11%
Totale		€ TOT																				
		4.201.616,34 €																				
Servizio infrastrutturale (canone bimestrale)		€ TOT																				
Infrastruttura - Secure Public Cloud	100%	85.825,06 €														16,67%	33,33%	16,67%	16,67%	33,33%	16,67%	33,33%
Infrastruttura - PSN Managed	100%	747.808,47 €								16,67%		16,67%		16,67%	16,67%	33,33%	16,67%	33,33%	16,67%	33,33%	16,67%	33,33%

Milestone di avanzamento €- Gate approvativi

			Anno 1												Anno 2				Anno 3			
Servizi di Migrazione (Milestone Based)	Peso	Importo	Month 1 - Startup	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		€ TOT																				
- Analisi & Discovery	30%	636.913,34 €	127.382,67 €	413.993,67 €	95.537,00 €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
- Setup	20%	424.608,89 €	- €	- €	- €	127.382,67 €	169.843,56 €	127.382,67 €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
- Migrazione	45%	955.370,00 €	- €	- €	- €	- €	- €	- €	95.537,00 €	143.305,50 €	143.305,50 €	238.842,50 €	143.305,50 €	143.305,50 €	47.768,50 €	- €	- €	- €	- €	- €	- €	- €
- Collaudo	5%	106.152,22 €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	10.615,22 €	95.537,00 €	- €	- €	- €	- €	- €	- €
Servizi professionali (canone mensile		€ TOT																				
- IT Service Operation	100%	1.742.990,20 €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	145.249,18 €	290.498,37 €	145.249,18 €	290.498,37 €	145.249,18 €	290.498,37 €	145.249,18 €	290.498,37 €
- Security Professional Services - Compliance Normativa	100%	194.982,45 €	- €	32.497,08 €	- €	32.497,08 €	- €	32.497,08 €	- €	32.497,08 €	- €	32.497,08 €	- €	32.497,08 €	- €	- €	- €	- €	- €	- €	- €	- €
- Security Professional Services - Supporto Sicurezza	100%	140.599,24 €	- €	7.811,07 €	- €	7.811,07 €	- €	7.811,07 €	- €	7.811,07 €	- €	7.811,07 €	- €	7.811,07 €	7.811,07 €	15.622,14 €	7.811,07 €	15.622,14 €	7.811,07 €	15.622,14 €	7.811,07 €	15.622,14 €
Totale		€ TOT	127.382,67 €	454.301,81 €	95.537,00 €	167.690,81 €	169.843,56 €	167.690,81 €	95.537,00 €	183.613,64 €	143.305,50 €	279.150,64 €	143.305,50 €	183.613,64 €	211.443,97 €	401.657,50 €	153.060,25 €	306.120,50 €	153.060,25 €	306.120,50 €	153.060,25 €	306.120,50 €
		4.201.616,34 €																				
Servizio infrastrutturale (canone bimestrale)		€ TOT																				
Infrastruttura - Secure Public Cloud	100%	85.825,06 €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	14.304,18 €	28.608,35 €	14.304,18 €	14.304,18 €	28.608,35 €	14.304,18 €	28.608,35 €
Infrastruttura - PSN Managed	100%	747.808,47 €	- €	- €	- €	- €	- €	- €	- €	124.634,75 €	- €	124.634,75 €	- €	124.634,75 €	124.634,75 €	249.269,49 €	124.634,75 €	249.269,49 €	124.634,75 €	249.269,49 €	124.634,75 €	249.269,49 €
Totale		€ TOT	127.382,67 €	454.301,81 €	95.537,00 €	167.690,81 €	169.843,56 €	167.690,81 €	95.537,00 €	308.248,39 €	143.305,50 €	403.785,39 €	143.305,50 €	308.248,39 €	336.078,72 €	665.231,17 €	306.303,35 €	569.694,17 €	291.999,17 €	583.998,35 €	291.999,17 €	583.998,35 €

Polo Strategico Nazionale

Di seguito viene riportata una tabella che sintetizza, per i primi tre anni, gli importi dei servizi professionali e del canone infrastrutturale suddivisi per anno:

	Anno 1	Anno 2	Anno 3		TOT 3 anni	
Migrazione Servizi	2.123.044,45 €	0,00 €	0,00 €		2.123.044,45 €	
IT Service Operation	0,00 €	839.623,46 €	903.366,74 €		1.742.990,20 €	
Security Professional Services	237.603,23 €	48.989,23 €	48.989,23 €		335.581,69 €	
Canone infrastruttura	373.904,24 €	805.025,18 €	833.671,47 €		2.012.600,89 €	
TOT SENZA IVA	2.734.551,92 €	1.693.637,87 €	1.786.027,44 €		6.214.217,23 €	
TOT CON IVA	3.336.153,34 €	2.066.238,20 €	2.178.953,48 €		7.581.345,02 €	

Le attività previste, sia di natura progettuale che continuativa, e il canone infrastrutturale nel periodo di tre anni, sono valutate per un totale pari a 6.214.217,23 € (IVA esclusa) (7.581.345,02 € comprensivo di IVA).

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 2024, il giorno XX del mese di giugno,

TRA

ASL Roma 1, con sede legale in Roma Borgo S. Spirito, 3, Codice Fiscale e Partita Iva n. 13664791004, nella persona del Legale Rappresentante, il Commissario Straordinario Dott. Giuseppe Quintavalle, domiciliato per la sua carica presso la sede legale dell'Azienda;

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. Emanuele Iannetti nato a Roma il 14 novembre 1967 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 **27/03/2024**, 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 **06/06/2024**, 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 **06/06/2024**, 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

15. Le attività svolte da PSN e dai soci sono configurabili di tipo intellettuali, non ricadenti sotto DUVRI.

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: **6BMH4**

18. Il CUP del presente Contratto è il seguente: **J81C23000670006**

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 xxx.

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 e fatto salve le variazioni che derivano da una modifica del Catalogo dei Servizi da parte del Concessionario

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, così come dettagliato nel Piano di migrazione di cui all'art. 7 .

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 ha prestato garanzia definitiva pari al 4% (quattro per cento) dell'importo del Contratto, salvo eventuali

riduzioni di cui all'art. 103 del **DLGS 50/2016** intervenute prima o successivamente alla stipula, rilasciata in data **<** [•] dalla società [•] avente numero [•] di importo pari ad euro [•] ([•]/00). ***da compilare a cura dell'Amministrazione>***

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 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.

3. Ai sensi dell'art. 176 DLGS 50/2016 alla risoluzione per inadempimento del concessionario si applica l'art. 1453 c.c. in base al quale è fatto salvo il risarcimento del danno subito dall'Amministrazione Utente.

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 giustificati motivi di pubblico interesse, risultanti da provvedimento amministrativo. Della revoca deve essere data 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 provvederà al pagamento in favore del Concessionario delle somme di cui all'art. 176, comma 4, nonché dei costi e delle penali da sostenere nei confronti di terzi, in conseguenza della risoluzione fermo restando quanto previsto al comma 5 del predetto art. 176 del Codice.

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 Borgo Santo Spirito, 3 - 00193 ROMA.

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 ***protocollo@pec.aslroma1.it.***

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 a cura e spese 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.

Azienda Sanitaria Locale Roma 1

Commissario Straordinario e Legale Rappresentate

Dott. Giuseppe Quintavalle

_____

Polo Strategico Nazionale S.p.A.

Amministratore Delegato

(Emanuele Iannetti)

_____

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)

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.

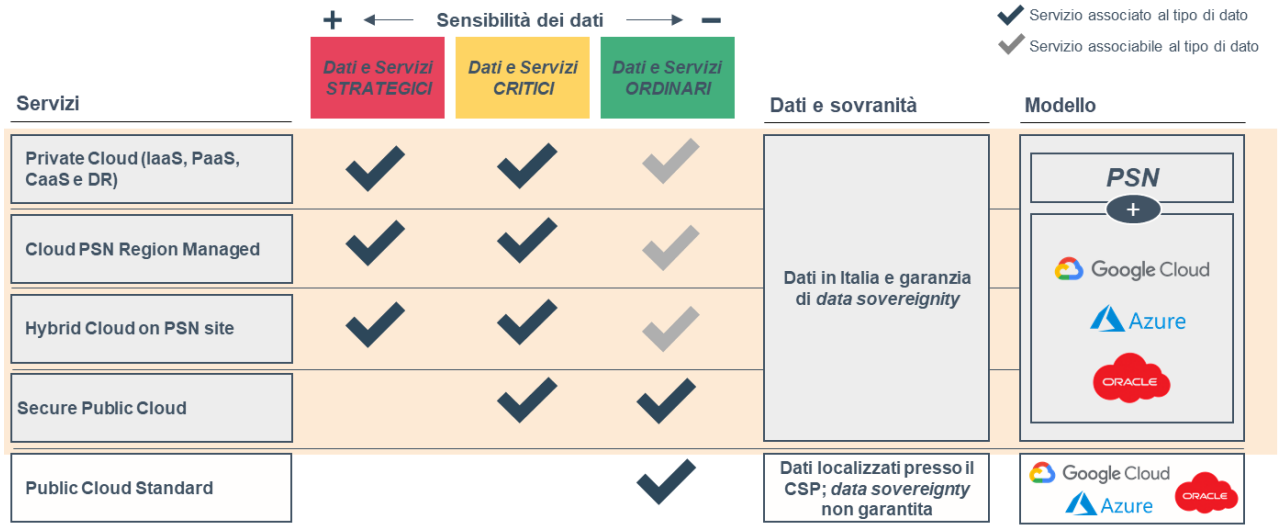
Glossario	Descrizione
PA	Pubbliche Amministrazioni
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
MTMS	Manuale tecnico sulle misure di sicurezza
Dati personali	Qualsiasi informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica e che possa fornire 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.

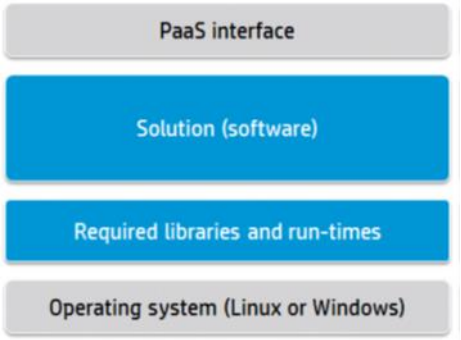
9.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

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: q**uesta 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

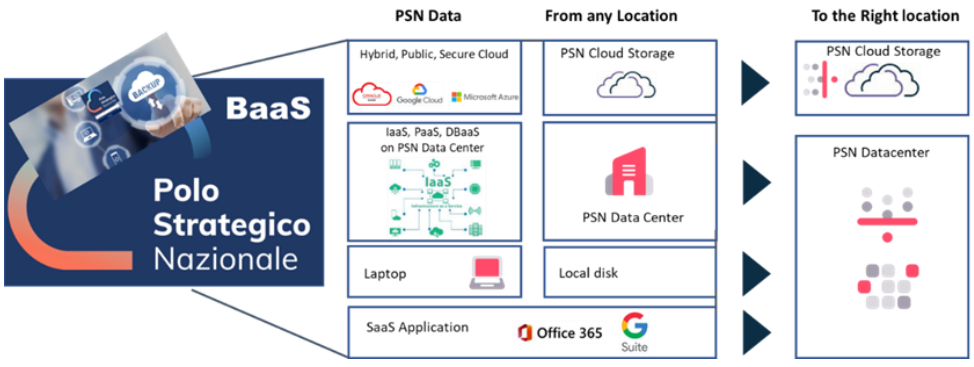
Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

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.

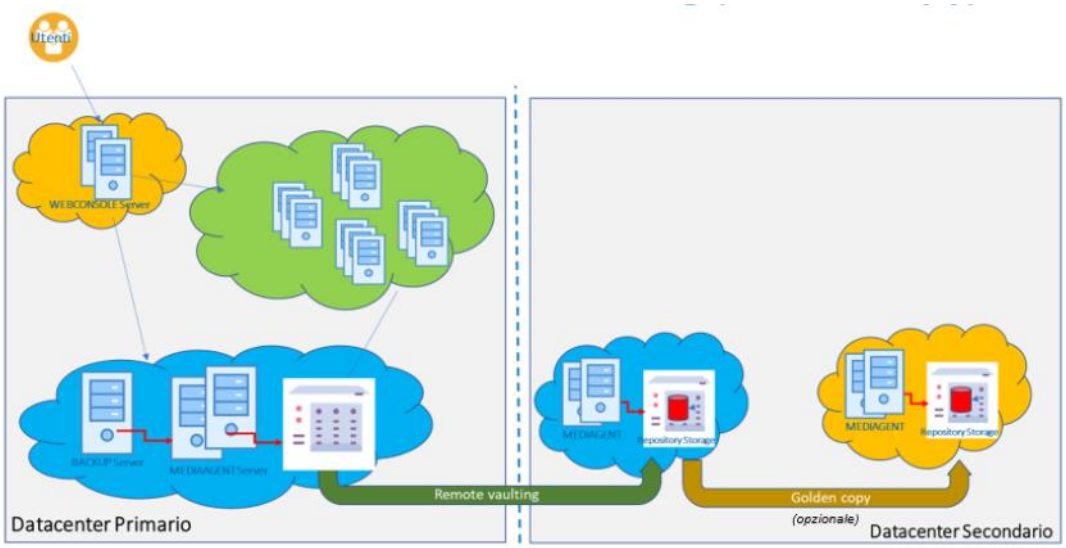
Tale servizio BaaS è erogato attraverso una console centralizzata attraverso la quale, in modalità self-managed, è possibile gestire la protezione dei vari contesti da proteggere (Files, VM, Container (k8), tutti i principali database come SAP-HANA, Exchange, SQL, Oracle, DB2, PostgreSQL, GPFS, MongoDB, 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

ll 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.

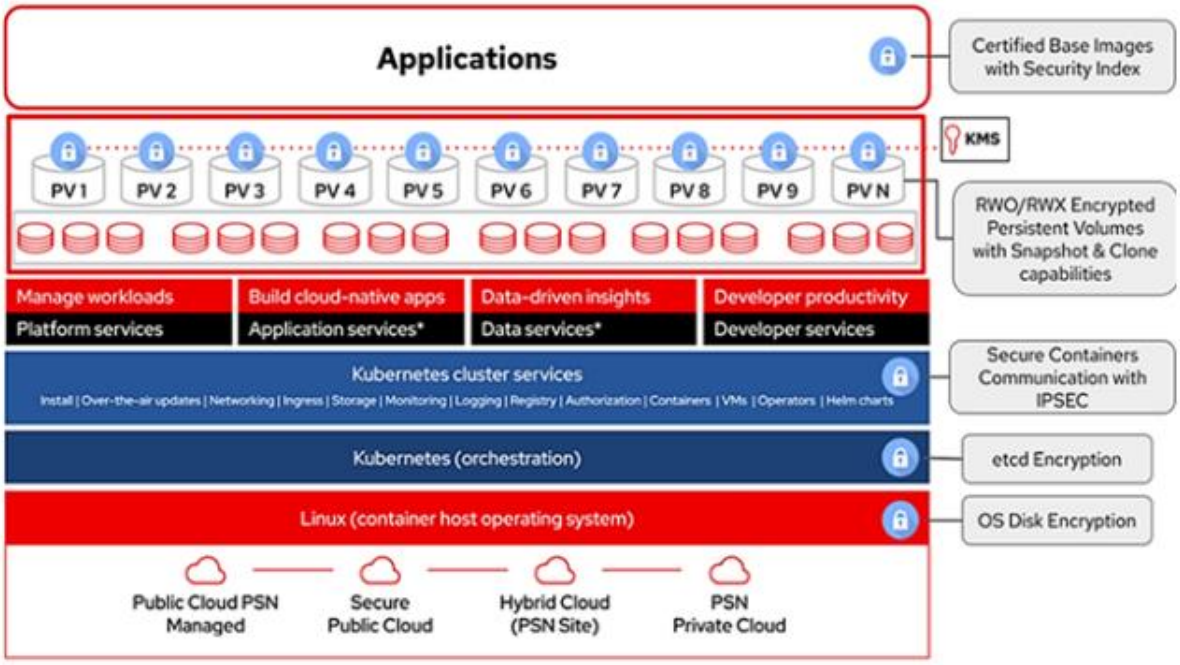
In particolare, per l'erogazione del servizio sarà utilizzata la distribuzione Red Hat di OpenShift, di cui OKD è il corrispondente progetto parallelo di community, su cui è basata appunto questa distribuzione: come per tutte le distribuzioni Red Hat, sul portale di accesso (access.redhat.com) è sempre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

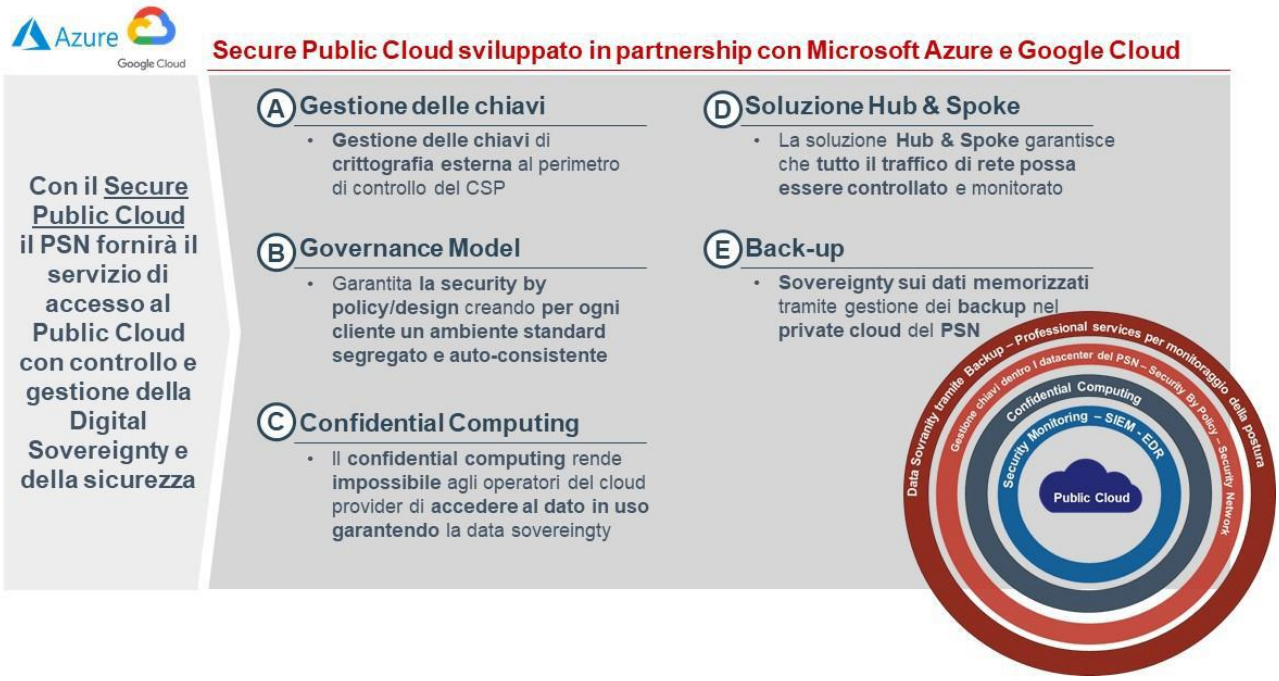
13.2 Secure Public Cloud

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)

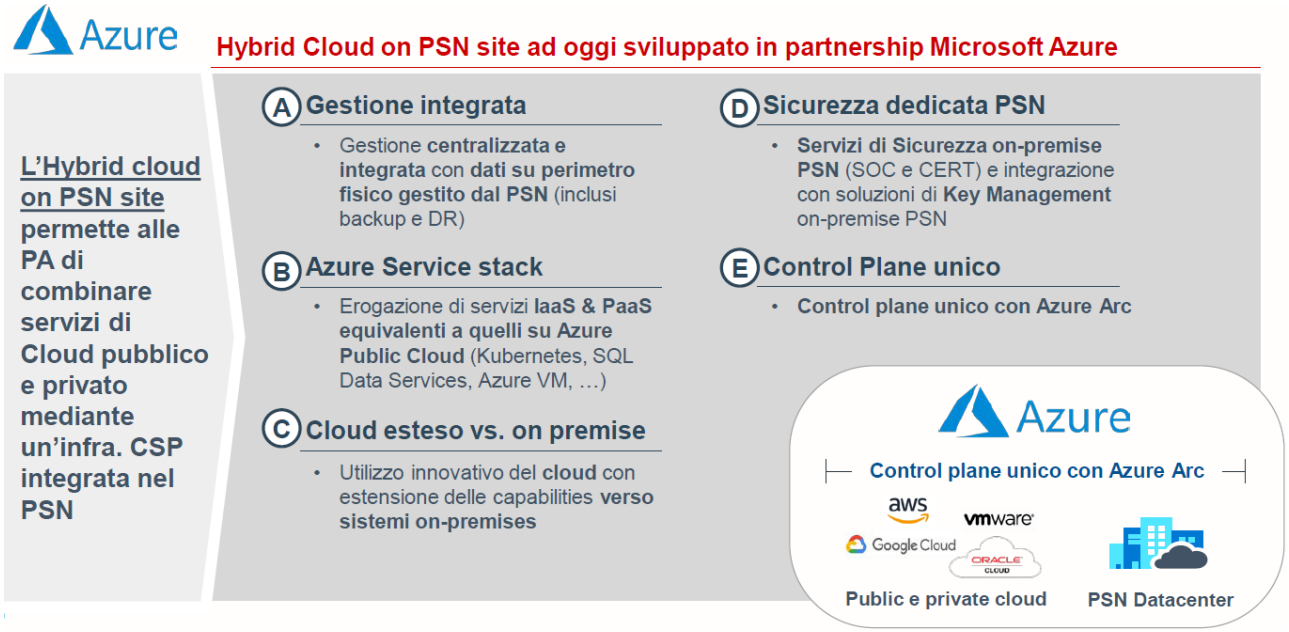
Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Google ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Google ed eventuali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

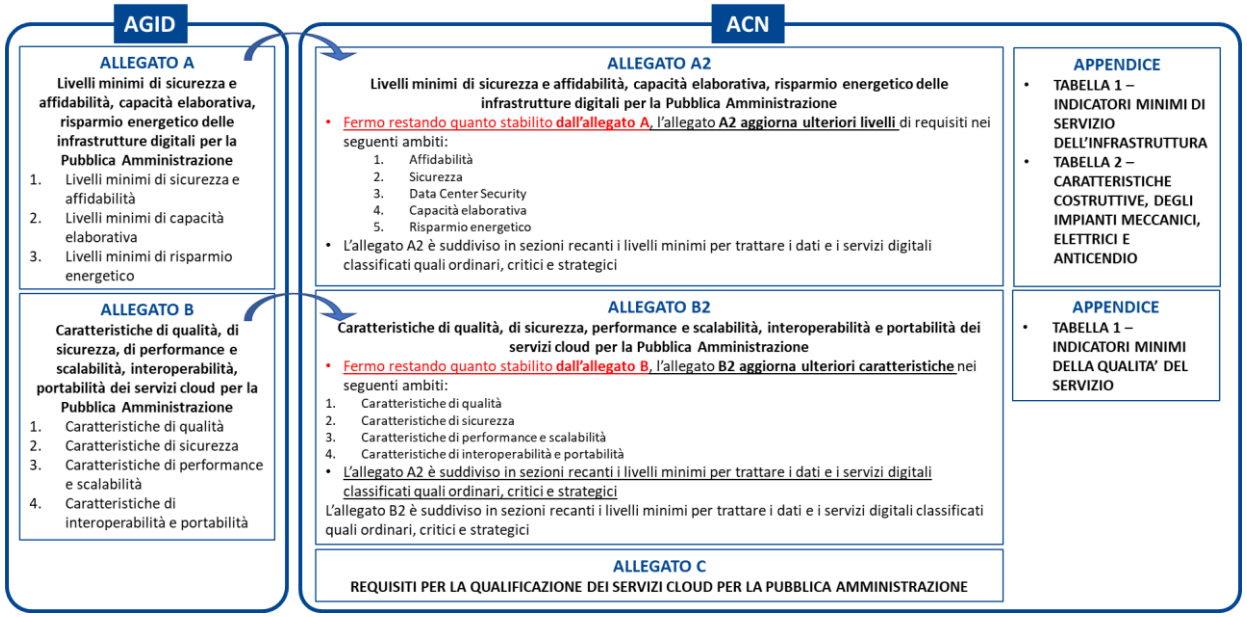
- Definizione **tipologia di qualifica:** qualifica di «**tipo C**» → **CSP /** qualifica di «**tipo A**» → **servizi IaaS/PaaS /** qualifica di «**tipo B**» → **servizi SaaS**

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 infrastruttura	
	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**
Critici	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 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)
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-provisioning 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

16.2.3.1 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 sotituto, 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 inguistificato 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 teminali (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 respondabilità 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 nonitoraggio, 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 l'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. Ilsoggetto 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

16.2.3.2 Requisiti Dati Critici

ID Requisito	Specifica Requisito
RS-AN-5	1. Gli esiti delle valutazioni di cui alla sottoocategoria 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 coinvolgono 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 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 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, nonchè 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. E 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 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 PRAC, PR.DS, PRA P e PR.MA e concorrono al rispetto delle politiche di cui alla categoria IDAM, 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.

16.2.3.3 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 coinvolgi mento 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, manutenuti 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 l 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 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, PRIP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, l D.SC, PR.AC e PRDS. 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti S 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. E 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.

16.2.4 Requisiti ACN-Allegato B2

16.2.4.1 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 respondabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2
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 nonitoraggio, 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 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.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. II 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 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 l'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 (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. Ilsoggetto 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.

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

16.2.4.2 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. E 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. II 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 contententente 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-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 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 PRAC, PR.DS, PRA P e PR.MA e concorrono al rispetto delle politiche di cui alla categoria IDAM, 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. II 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.

16.2.4.3 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. E 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		
Livello	**Caratteristiche dei servizi**	**Certificazioni**
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.
Ulteriori requisiti per la qualificazione cloud di livello 4		

ID Caratteristica Specifica	Caratteristica specifica	ID Requisito	Nome	Specifica Requisito
5.1.1.	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
5.1.2.	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. E 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.
5.1.3.	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		
Livello	**Livelli minimi delle infrastrutture digitali**	**Certificazioni**
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.

Ulteriori requisiti per la qualificazione infrastruttura di livello 4				
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.

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 n 2024-0000013664791004-PPdF-P1R1 del 05/06/2024 - 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 19.204.443,43 (€ diciannovemilioniduecentoquattromilaquattrocentoquarantatre/43) 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 768.177,74 (€ settecentosessantottomilacentosettantasette/74).

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 data di 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, sino alla completa esecuzione del Contratto medesimo.

Si prega pertanto di consegnare la garanzia definitiva entro 3 giorni lavorativi dal ricevimento della presente richiesta.

Cordiali saluti

Il Commissario Straordinario

Dott. Giuseppe Quintavalle

Data 10/06/2024