REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO SALUTE E WELFARE
SETTORE 5 - ASSISTENZA OSPEDALIERA E SISTEMI ALTERNATIVI AL RICOVERO

Assunto il 18/03/2025

Numero Registro Dipartimento 392

==========

DECRETO DIRIGENZIALE

"Registro dei decreti dei Dirigenti della Regione Calabria"

N°. 4346 DEL 26/03/2025

Settore Gestione Entrate	Settore Ragioneria Generale – Gestione Spese
VISTO di regolarità contabile, in conformità all'allegato 4/2 del D.lgs. n. 118/2011 **Sottoscritto dal Dirigente del Settore** Dott.STEFANIZZI MICHELE (con firma digitale)	VISTO di regolarità contabile attestante la copertura finanziaria, in conformità all'allegato 4/2 del D.lgs. n. 118/2011 **Sottoscritto dal Dirigente del Settore** Dott. GIORDANO UMBERTO ALESSIO (con firma digitale)

Oggetto: 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. Affidamento - Accertamenti e Impegni anni 2025 - 2026 - 2027

IL DIRIGENTE GENERALE

VISTI:

- la Legge 7 agosto 1990 n. 241 e ss.mm.ii., recante norme sul procedimento amministrativo;
- Il D. Lgs. n. 502 del 1992 “Riordino della disciplina in materia sanitaria, a norma dell’art.1 della L. 23 ottobre 1992 n. 421;
- la Legge regionale 13 maggio 1996, n. 7, recante “Norme sull’ordinamento della struttura organizzativa della Giunta Regionale e sulla dirigenza regionale”;
- Il D. Lgs. n. 229 del 19 giugno 1999 “Norme per la razionalizzazione del Servizio Sanitario Nazionale, a norma dell’art. 1 della legge 30 novembre 1998, n. 419’’;
- il D.P.G.R. n.354 del 24 giugno 1999 concernente la separazione dell’attività amministrativa di indirizzo e di controllo da quella gestionale, modificato con D.P.G.R. 206 del 15 dicembre 2000;
- il D.C.A. n.162 del 18/11/2022 con il quale è stato approvato il Programma Operativo 2022/2025
- il D.Lgs. 7 marzo 2005, n. 82;
- il D.Lgs. n. 50 del 18.04.2016 e ss.mm.ii.;
- il D. Lgs n. 36/2023;
- la D.G.R. n. 665 del 14 dicembre 2022, avente ad oggetto: “Misure per garantire la funzionalità della struttura organizzativa della Giunta Regionale - Approvazione Regolamento di riorganizzazione delle strutture della Giunta Regionale. Abrogazione regolamento regionale 20 aprile 2022, n.3 e ss.mm.ii”;
- il Regolamento Regionale n. 12/2022 recante “Regolamento di organizzazione delle strutture della Giunta Regionale” approvato con DGR n.665 del 14 dicembre 2022;
- la L.R. 1° dicembre 2022, n. 42, recante “Riordino del sistema dei controlli interni e istituzione dell’Organismo regionale per i controlli di legalità”;
- la D.G.R. n. 3 del 12 gennaio 2023, recante “Regolamento delle procedure di controllo interno in attuazione dell’articolo 4, comma 7 e dell’articolo 9 della legge regionale 1dicembre 2022, n. 42 (Riordino del sistema di controlli interni e istituzione dell’Organismo regionale per i controlli di legalità)”;
- la D.G.R. n. 29 del 06/02/2024 - Approvazione Piano Integrato di Attività e Organizzazione (PIAO) 2024/2026 per come modificata ed integrata con la DGR n. 444 del 12/08/2024;
- la Circolare Prot. N. 765486 del 05/12/2024 ad oggetto: "D.G.R. n. 536 del 19/10/2024 “Approvazione Piano dei controlli di regolarità amministrativa in fase successiva – Anno 2025”. Disposizioni operative";
- la D.G.R. del 24 ottobre 2024, n. 572, recante “Misure per garantire la funzionalità della struttura organizzativa della Giunta Regionale – approvazione modifiche del regolamento Regionale n. 12/2022 e s.m.i.”;
- il Regolamento Regionale n. 11/2024 recante “Modifica del Regolamento di organizzazione delle strutture della Giunta Regionale n. 12/2022”;
- la D.G.R. del 24 ottobre 2024, n. 572 e successivo D.P.G.R. n. 69 del 24 ottobre 2024 con cui è stato conferito al Dott. Tommaso Calabrò - Dirigente di ruolo della Giunta della Regione Calabria - l’incarico di Dirigente generale ad interim del Dipartimento “Salute e Welfare” nelle more dell’espletamento delle procedure di legge per l’individuazione del Dirigente titolare, per la durata, ai sensi dell’art. 10 del RR n. 11/2021 e s.m.i, di anni uno, salva l’estinzione anticipata per effetto della nomina del titolare;
- il D.D.G. n. 15682 del 08/11/2024 con cui è stata approvato il provvedimento di micro-organizzazione relativo ai Settori/UOA del Dipartimento “Salute e Welfare”;
- il D.D.G. n. 15985 del 14/11/2024 recante “D.D.G. n. 15682 del 08.11.2024 - integrazione, modifica e riapprovazione dell’Allegato 2);

VISTI, altresì:

- Il D.lgs. n 118/2011 contenente disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli Enti Locali e dei loro Organismi;
- la Legge Regionale n. 41 del 23/12/2024 avente ad oggetto “Legge di stabilità regionale 2025”;
- la Legge Regionale n. 42 del 23/12/2024 avente ad oggetto “Bilancio di previsione finanziario della Regione Calabria per gli anni 2025 – 2027”;
- la Deliberazione di Giunta Regionale n. 766 del 27/12/2024 “Documento tecnico di accompagnamento al bilancio di previsione finanziario della Regione Calabria per gli anni 2025 – 2027 (artt. 11 e 39, c. 10, d.lgs. 23/06/2011, n. 118)”;

- la Deliberazione di Giunta Regionale n. 767 del 27/12/2024 "*Bilancio finanziario gestionale della Regione Calabria per gli anni 2025 – 2027 (art. 39, c. 10, d.lgs. 23/06/2011, n. 118)*";

VISTI, ancora:

- Il DCA n.13 del 25/02/2022 avente ad oggetto "Piano di recupero per le liste d'attesa, ai sensi della legge 30 dicembre 2021, n. 234 - articolo 1, commi 276 e 279."
- Il DCA n. 45 del 20/04/2022 avente ad oggetto" Implementazione e ammodernamento delle infrastrutture tecnologiche legate ai sistemi di prenotazione elettronica per l'accesso alle strutture sanitarie" con cui il Dipartimento Tutela della Salute e Servizi Socio Sanitari è stato autorizzato all'adesione all'Accordo Quadro per l'affidamento di Servizi applicativi di Data Management per le Pubbliche Amministrazioni, ID 2102- LOTTO 3, CIG 8184365FA4, presente sulla piattaforma CONSIP;
- Il DCA n. 162 del 18 novembre 2022 avente ad oggetto: "Approvazione Programma Operativo 2022-2025 predisposto ai sensi dell'articolo 2 comma 88, della L 23 dicembre 2009 num. 191 ed s.m.i.";
- Il DCA n. 3 del 11/01/2024 avente ad oggetto: "Approvazione ed adozione delle Linee Guida del CUP della Calabria";
- il DCA n. 287 del 1 ottobre 2024 recante "DCA n. 52 del 23 febbraio 2024 - Passaggio delle funzioni afferenti alla Struttura complessa I.C.T., Infrastrutture e Applicativi digitali, Coordinamento e Gestione dei flussi informativi, dalle Aziende del Servizio Sanitario Calabrese all'Azienda per il Governo della Sanità della Regione Calabria – Azienda Zero" in cui tra l'altro è disposta la presa d'atto della conclusione del procedimento di attuazione del passaggio delle funzioni afferenti alla Struttura complessa I.C.T., Infrastrutture e Applicativi digitali, Coordinamento e Gestione dei flussi informativi, dalle Aziende del Servizio Sanitario Calabrese all'Azienda per il Governo della Sanità della Regione Calabria – Azienda Zero, così come disciplinato dal Regolamento approvato con il D.C.A. n. 52/2024;

PREMESSO che:

- La Regione Calabria, nell'ambito della riorganizzazione e dell'evoluzione del sistema CUP, si è posta l'obiettivo di realizzare un CUP regionale scegliendo di applicare il modello del CUP interaziendale su scala regionale - d'ora in poi definito SovraCUP - attraverso l'adozione di una specifica soluzione applicativa che sarà utilizzata all'interno del Sistema Sanitario Regionale.
- VALIDA (VAlutazione LIste Di Attesa) è il Progetto di informatizzazione con cui la Regione ha introdotto e reso note e pervasive le piattaforme abilitanti per la gestione e il controllo delle liste di attesa e per l'analisi proattiva dei dati sanitari, con particolare focus sulla gestione di tutte le fattispecie legate al processo di prenotazione di prestazioni sanitarie;
- Con VALIDA è stato istituito il SovraCUP Regionale Unico che ha definitivamente sancito un passaggio da un modello statico ad un modello di gestione delle prenotazioni di tipo misto, nel senso che conserva l'operatività degli attuali CUP Aziendali (Area Nord, Centro e Sud) ai quali affianca un mainframe - SovraCUP Regionale Unico - che accentra soltanto alcune delle funzionalità attualmente gestite dai CUP Aziendali (essenzialmente, gestione delle agende e delle prenotazioni);
- Il SovraCUP Regionale Unico è destinato alla prenotazione di prestazioni sanitarie di specialistica ambulatoriale a carico del Servizio Sanitario Nazionale (SSN) e in libera professione intramoenia, nonché di quelle previste da programmi nazionali e regionali di prevenzione erogate da strutture sanitarie pubbliche, private contrattualizzate e presidi equiparati;
- Il modello complessivo si articola su tre livelli logici ed ha portato, nel corso delle ultime due annualità, su infrastruttura a disposizione della regione Calabria, alla realizzazione di un SovraCUP Unico per mezzo del quale sono gestite tutte le agende, formate dalle disponibilità delle risorse che le Aziende mettono a disposizione per i pazienti e che vengono rese prenotabili anche da altre aziende (agende globali) e dalle agende che le Aziende mantengono per le proprie necessità interne (agende pubbliche e private);
- L'insieme dei servizi attualmente erogati fa capo ad un sistema gestionale realizzato con tecnologia Java e sui canali che espongono tutte le funzionalità all'utenza finale;
- Oltre al sistema gestionale, ad oggi è possibile erogare i servizi grazie ad un impianto composto da Portale Regionale delle Liste di Attesa e di Prenotazione e APP per il Cittadino;

VISTA la Convenzione del 24/08/2022, stipulata ai sensi degli artt.164, 165, 179, 180, comma 3 e 183, comma15 del D.Lgs.18 aprile 2016, n.50 tra la Presidenza del Consiglio dei Ministri–Dipartimento per

la Trasformazione Digitale e la Società Polo Strategico Nazionale S.p.A ("PSN S.p.A") società di costituzione partecipata da TIM, Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei, avente a oggetto l'affidamento in concessione della realizzazione del progetto de quo attraverso l'utilizzo dei servizi PSN" è stata affidata in concessione, per la durata di 13 anni, la progettazione, realizzazione e gestione dell'infrastruttura per l'erogazione di servizi cloud per la Pubblica Amministrazione;

VISTO il DCA n. 20 del 28/01/2025 avente ad oggetto "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. Atto di indirizzo" ove è stato dato atto che:

- la Regione Calabria, nell'ambito di un percorso di innovazione ed efficienza delle infrastrutture tecnologiche ed informatiche, intende avvalersi della nuova infrastruttura Cloud PSN per disporre di ambienti caratterizzati da maggiore sicurezza, autonomia e alta affidabilità;
- si rende necessaria l'aggregazione del Portale Regionale delle Liste di Attesa e di Prenotazione e APP per il Cittadino insieme al resto dei servizi dedicati all'utenza sanitaria, all'interno di un solo ed unico cruscotto o portale della Sanità Regionale Calabrese;

DATO ATTO che con il summenzionato DCA:

- è stato dato indirizzo al Dipartimento Salute e Welfare, in continuità con la precedente progettualità allo stesso affidata con DCA n. 45 del 20/04/2022, di predisporre ed attuare di quanto necessario per la realizzazione del progetto di migrazione su infrastruttura Cloud PSN e per l'aggregazione del Portale Regionale delle Liste di Attesa e di Prenotazione e APP per il Cittadino insieme al resto dei servizi dedicati all'utenza sanitaria, all'interno di un solo ed unico cruscotto o portale della Sanità Regionale Calabrese;
- È stato statuito che l'attuazione della progettualità verrà svolta in sinergia con l'Azienda per il Governo della Sanità della Regione Calabria – Azienda Zero;

PRESO ATTO che la procedura in esame costituisce un'acquisizione diretta di servizi mediante l'adesione alla Convenzione PSN, prevedendo che l'acquisizione possa essere effettuata rivolgendosi direttamente alla Società di Progetto (Concessionario della Convenzione) denominata Polo Strategico Nazionale Spa, tramite presentazione da parte dell'Amministrazione del Piano dei fabbisogni e, a seguito della successiva approvazione del Progetto dei fabbisogni, da perfezionarsi tramite stipula del contratto d'Utenza, e che alla medesima procedura deve intendersi applicabile quanto previsto dalla normativa vigente in materia di contratti pubblici al momento della sottoscrizione della predetta Convenzione PSN di concessione del 24 agosto 2022;

CONSIDERATO che:

- Il Dipartimento Salute e Welfare, con PEC del 17/09/2024, in atti, in conformità a quanto disposto dall'art. 18 della sopra citata Convenzione, ha inviato al PSN il Piano dei Fabbisogni;
- il PSN, a seguito della formalizzazione del Piano dei Fabbisogni di cui alla sopra citata Convenzione, effettuata in data 15/10/2024 ha comunicato con nota pec del 17/10/2024, in atti, la presa in carico della richiesta a cui è stato assegnato il codice n. 2024-0000002205340793-PdF-P9R1;
- il Polo Strategico Nazionale S.p.A (PSN S.p.A.), ha trasmesso in data 22/11/2024 a mezzo pec il Progetto del piano dei fabbisogni "2024-0000002205340793-PPdF-P8R1", contenente la descrizione dei servizi e la relativa quantificazione economica secondo le modalità tecniche ed i listini previsti nella Convenzione di Concessione e nei relativi allegati;
- con comunicazione PEC di pari data PSN S.p.A. ha trasmesso il contratto d'utenza contenente la clausola di recesso anticipato;

PRECISATO che:

- i servizi da acquistare possiedono caratteristiche di base conformi agli standard definiti dall'Amministrazione regionale, rispettando le esigenze prioritarie espresse dalla stessa;
- per quanto sopra, l'acquisto dei servizi richiesti di che trattasi verrà effettuato in via telematica mediante la stipula di un contratto di utenza, di cui allo schema sopra citato;
- occorre procedere all'approvazione del Progetto del Piano dei Fabbisogni - identificativo "2024-0000002205340793-PPdF-P8R1";
- sono stati acquisiti il CIG 9066973ECE, e il GIG derivato B5F978E27D;

DATO ATTO che:

- l'importo per l'acquisizione dei servizi ammonta euro 9.635.959,17 IVA esclusa per l'intera

durata contrattuale (36 mesi) a valere sulle risorse del fondo sanitario indistinto;

- l'importo degli incentivi tecnici ammonta ad euro 192.719,18 pari al 2% dell'importo del servizio che trova copertura sul medesimo capitolo di spesa previsto per il servizio; in particolare della suddetta somma l'80% (pari a euro 154.175,34) per le spese di corresponsione degli incentivi e il restante 20% (euro 38.543.84), trattandosi di fondi a destinazione vincolata, costituisce una economia e confluisce nel quadro economico;
- che il quadro economico del progetto, pari ad euro 11.755.870,19 è così composto:

QUADRO ECONOMICO				
A) Servizio	*Anno 2025*	*Anno 2026*	*Anno 2027*	TOTALE
a.1 - Valida 2	€ 4.357.321,01	€ 3.113.103,42	€ 2.165.534,74	€ 9.635.959,17
a2 - IVA (22%)	€ 958.610,62	€ 684.882,75	€ 476.417,64	€ 2.119.911,02
Totale Importo Lavori oggetto di Appalto	***€ 5.315.931,63***	***€ 3.797.986,17***	***€ 2.641.952,38***	**€ 11.755.870,19**
B) Incentivi per funzioni tecniche	€ 87.146,42	€ 62.262,07	€ 43.310,70	**€ 192.719,18**
TOTALE IMPORTO (A) + (B)	**5.403.078,05**	**3.860.248,24**	**€ 2.685.263,08**	**€ 11.948.589,37**

- la somma complessiva pari euro 11.948.589,37 sarà imputata sul capitolo di spesa U0421110306 che presenta adeguata disponibilità;

CONSIDERATO che gli incarichi di RUP e DEC, possono essere conferiti a dipendenti a tempo indeterminato e determinato dell'Amministrazione Regionale, nonché a dipendenti di altre amministrazioni in posizione di comando o di temporaneo utilizzo presso l'Amministrazione regionale,

DATO ATTO che**:**

- con nota prot.105710 del 18/02/2025, in atti, si è provveduto alla nomina quale Responsabile Unico del Progetto il funzionario Aurelio Zaccone, dipendente dell'ASP di Catanzaro in servizio presso il Dipartimento Salute e Welfare, in possesso della competenza richiesta e quali supporti al RUP i funzionari Leopoldo Bilotti e Anna Liconti, in servizio presso Dipartimento Salute e Welfare;
- con nota prot. 105727 del 18/02/2025, in atti, si è provveduto alla nomina quale DEC dell'ing. Francesco Curia in servizio Dipartimento Transizione Digitale e Attività Strategiche e quali supporti al DEC, dell'ing. Anna Garasto e dell'ing. Fabio Maria Catalano in servizio Dipartimento Transizione Digitale e Attività Strategiche,
- Con successiva nota prot. 141439 del 05/03/2025 si è individuato, quale ulteriore supporto al DEC, il dipendente Michelangelo Rossano, in servizio presso Dipartimento Salute e Welfare;

RITENUTO di riconoscere al RUP, al DEC e al personale con funzione di supporto tecnico/amministrativo sopra indicati, ai sensi della normativa vigente, gli incentivi per funzioni tecniche nei limiti del fondo appositamente previsto nel quadro economico dell'intervento;

RITENUTO, pertanto:

- di aderire alla Convenzione PSN suddetta per la fornitura dei servizi richiesti e precisamente:
  - Industry standard Hosting
  - Industry standard – Housing
  - Industry standard IaaS
  - Industry standard PaaS
  - Industry standard CaaS
  - Public Cloud PSN Managed
  - Servizi di migrazione
  - Servizi professionali - Servizio Re-Architect
  - Servizi professionali - Servizio Re-Platform
  - Servizi professionali - Security Professional Services
  - Servizi professionali - IT Infrastructure - Service Operations
  - Altri servizi a listino:

Ambiente	Hostname	vCPU	RAM	Storage	Storage Data	OS	Note
Pre-Prod	cvalida-lx-lbc01	2	4	50		RHEL 8.x	
Pre-Prod	cvalida-lx-appl01	4	48	100		RHEL 8.x	
Pre-Prod	cvalida-lx-appl02	4	48	100		RHEL 8.x	
Pre-Prod	ENG-VALIDA-DB-PreProd	8	32	300	4.000		Base DB Server Oracle BYOL
DWH	dvalida-lx-lbc01	2	4	50		RHEL 8.x	
DWH	dvalida-lx-appl01	8	32	100		RHEL 8.x	
DWH	dvalida-lx-appl02	8	32	100		RHEL 8.x	
DWH	ENG-VALIDA-DB-DWH	16	32	300	4.000		Base DB Server Oracle BYOL
Test	tvalida-lx-lbc01	2	4	50		RHEL 8.x	
Test	tvalida-lx-appl01	4	32	100		RHEL 8.x	
Test	tvalida-lx-appl02	4	32	100		RHEL 8.x	
Test	tvalida-lx-appl03	4	32	100		RHEL 8.x	
Test	tvalida-lx-WSO2-EII	8	16	100		RHEL 8.x	
Test	tvalida-lx-WSO2-DAS	4	16	100		RHEL 8.x	
Test	ENG-VALIDA-DB-Test	8	32	300	4.000		Base DB Server Oracle BYOL
Produzione	pvalida-lx-lbc01	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc02	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc03	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc04	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-appl01	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl02	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl03	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl04	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl05	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl06	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl07	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl08	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl09	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl10	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl11	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl12	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl13	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl14	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl15	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl16	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl17	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl18	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-WSO2-EII-1	8	32	200		RHEL 8.x	
Produzione	pvalida-lx-WSO2-EII-2	8	32	200		RHEL 8.x	
Produzione	pvalida-lx-WSO2-DAS	12	32	1.024		RHEL 8.x	
Produzione	pvalida-lx-zabbix	8	16	400		RHEL 8.x	
Produzione	ENG-VALIDA-DB-Prod1	48	128	300	4.000		Base DB Server Oracle BYOL
Produzione	ENG-VALIDA-DB-Prod2	48	128	300			Base DB Server Oracle BYOL
		370	**1932**	**6374**	**16000**		

Per i quali PSN SpA ha proposto soluzioni individuate per soddisfare le esigenze dell'Amministrazione sintetizzate nella tabella che segue:

Servizio	Tipologia
Public Cloud PSN Managed	Oracle Cloud
Servizi di Migrazione	
Servizi Professionali	Re-Architect
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

- di procedere all'approvazione Progetto del Piano dei Fabbisogni - identificativo "2024-0000002205340793-PPdF-P8R1" per un periodo contrattuale 36 mesi per l'importo di € 11.755.870,19 IVA inclusa
- di approvare lo schema di contratto di utenza, inviato dal Polo Strategico Nazionale S.p.A con

pec del 22 novembre 2024;

VISTA la Deliberazione di Giunta Regionale n. 70 del 28/02/2025 avente ad oggetto "*Variazione al documento tecnico di accompagnamento e al bilancio finanziario gestionale nell'ambito dei capitoli del fondo sanitario regionale (nota n. 108613 del 19.02.2025)*."

RITENUTO pertanto, di accertare e di impegnare le somme di cui al quadro economico per le annualità 2025, 2026 e 2027, come da prospetto sotto riportato;

Anno	ENTRATA		SPESA			
			Servizio			
	Importo (€)	Accertamento cap. di entrata E0120210801	Importo con IVA (€)	Impegno cap. di spesa U0421110306	Importo (€)	Impegno – cap. di spesa U0421110306
2025	5.403.078,05	2043/2025	5.315.931,64	3663/2025	28.624,18	3731/2025 (ASP CZ)
					41.092,95	3660/2025 (REG. CALABRIA)
					17.429,28	3666/2025 (GSA)
2026	3.860.248,24	371/2026	3.797.986,17	399/2026	14.944,22	409/2026 (ASP CZ)
					34.865,44	398/2026 (REG.CALABRIA)
					12.452,41	400/2026 (GSA)
2027	2.685.263,08	236/2027	2.641.952,38	217/2027	10.392,96	225/2027 (ASP CZ)
					24.255,60	216/2027(REG.CALABRIA)
					8.662,14	218/2027 (GSA)
TOTALE	11.948.589,37		11.755.870,19		192.719,18	

VISTE

- le proposte di accertamento nn. 2043/2025, nn.371/2026 e 236/2027, capitolo di entrata E012210801, generate telematicamente tramite la procedura COEC, assunte con il presente decreto di cui costituiscono parte integrante e sostanziale;
- le proposte di impegno nn. 3660/2025 - 3663/2025 – 3666/2025,- . 3731/2025 – nn- 398/2026 – 399/2026 – 400/2026, nn. 409/2026, nn. 216/2027 – 217/2027 – 218/2027 – 225/2027 capitolo di spesa U0421110306, generate telematicamente tramite la procedura COEC, e assunte con il presente decreto di cui costituiscono parte integrante e sostanziale;

ATTESTATO che:

- ricorrono i presupposti per procedere all'assunzione dell'impegno, ai sensi delle disposizioni previste dall'art.56 e dal paragrafo 5 dell'allegato 4/2 del D.Lgs. n. 118/2011;
- ai sensi dell'art. 4 della legge regionale n. 47/2011, per l'impegno di che trattasi, è stata riscontrata la necessaria copertura finanziaria sul pertinente capitolo U0421110306 e la corretta imputazione della spesa sul bilancio degli esercizi finanziari 2025-2026-2027;

CONSIDERATO che l'obbligazione giuridica correlata al presente provvedimento è perfezionata, in quanto sono determinate le somme da pagare, i soggetti creditori, la ragione dei debiti nonché la scadenza dell'obbligazione e che, pertanto, occorre costituire vincolo sulle previsioni di bilancio, nell'ambito della disponibilità finanziaria

SU PROPOSTA del Responsabile unico di progetto che attesta la regolarità amministrativa nonché la correttezza e la legittimità del presente atto;

DECRETA

per le motivazioni espresse in narrativa e che qui si intendono integralmente riportate:

DI DETERMINARSI A CONTRARRE, ai sensi di legge, per la realizzazione del progetto "Migrazione al PSN del Sistema VALIDA (VAlutazione LIste Di Attesa)" In Adesione Al Polo Strategico Nazionale (PSN);

DI ADERIRE, ai sensi di legge, per la realizzazione del progetto di che trattasi, alla Convenzione della Presidenza del Consiglio dei Ministri–Dipartimento per la Trasformazione Digitale– del 24/08/2022, stipulata ai sensi degli artt.164, 165, 179, 180, comma 3 e183, comma15 del D.Lgs.18 aprile 2016, n.50 e s.m.i., avente a oggetto l'affidamento in concessione della realizzazione del progetto de quo attraverso l'utilizzo dei servizi PSN" di cui al comma 1 dell'articolo 33-septies del d.l.n.179 del 2012. CUP: J51F24000060007–CIG:9066973ECE;

DI APPROVARE i documenti allegati al presente atto, finalizzati all'attivazione della procedura di adesione alla Convenzione PSN e propedeutici al perfezionamento dell'acquisizione dei servizi di interesse ed in particolare:

- il Progetto del Piano dei Fabbisogni "2024-0000002205340793-PPdF-P8R1", contenente la descrizione dei servizi e la relativa quantificazione economica secondo le modalità tecniche ed i listini previsti nella Convenzione di Concessione e nei relativi allegati, pervenuto per mezzo PEC del 22/11/2024, per la realizzazione del progetto di che trattasi, trasmesso dal Polo Strategico Nazionale S.p.A (PSN S.p.A.), società di costituzione partecipata da TIM, Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei;
- lo schema di contratto di utenza, inviato dal Polo Strategico Nazionale S.p.A con PEC del 22/11/2024;

DI DARE ATTO che l'importo per l'acquisizione dei servizi ammonta € 11.755.870,19 IVA inclusa per l'intera durata del progetto (36 mesi) a valere sul capitolo di bilancio U0421110306;

DI APPROVARE il quadro economico del progetto pari ad € **11.948.589,37** (iva inclusa), così ripartito:

QUADRO ECONOMICO				
A) Servizio	*Anno 2025*	*Anno 2026*	*Anno 2027*	TOTALE
a.1 - Valida 2	€ 4.357.321,01	€ 3.113.103,42	€ 2.165.534,74	€ 9.635.959,17
a2 - IVA (22%)	€ 958.610,62	€ 684.882,75	€ 476.417,64	€ 2.119.911,02
Totale Importo Lavori oggetto di Appalto	*€ 5.315.931,63*	*€ 3.797.986,17*	*€ 2.641.952,38*	€ 11.755.870,19
B) Incentivi per funzioni tecniche	€ 87.146,42	€ 62.262,07	€ 43.310,70	€ 192.719,18
TOTALE IMPORTO (A) + (B)	5.403.078,05	3.860.248,24	€ 2.685.263,08	€ 11.948.589,37

DI CONFERMARE:

- la nomina, disposta con nota prot. 105710 del 18/02/2025, in atti, del funzionario Aurelio Zaccone, in servizio presso il Dipartimento Salute e Welfare, quale Responsabile Unico del Progetto, nonché le nomine dei funzionari Leopoldo Bilotti e Anna Liconti, in servizio presso Dipartimento Salute e Welfare, quali supporti al RUP;
- la nomina, disposta con nota prot. 105727 del 18/02/2025, in atti, dell'ing. Francesco Curia in servizio Dipartimento Transizione Digitale e Attività Strategiche, quale DEC, nonché le nomine dell'ing. Anna Garasto e dell'ing. Fabio Maria Catalano in servizio Dipartimento Transizione Digitale e Attività Strategiche, quali supporti al DEC;
- la nomina, disposta con nota prot. 141439 del 05/03/2025 del dipendente Michelangelo Rossano, quale supporto al DEC;

DI RICONOSCERE al RUP, al DEC e al personale con funzione di supporto tecnico/amministrativo sopra indicati, ai sensi della normativa vigente, gli incentivi per funzioni tecniche nei limiti del fondo appositamente previsto nel quadro economico dell'intervento;

DI DARE ATTO CHE il Dipartimento Salute e Welfare, relativamente alla corresponsione degli incentivi, provvederà alla liquidazione e all'ammissione del mandato di pagamento sul capitolo U0421110306 a cui farà seguito una reversale di incasso, effettuata dal competente Settore del dipartimento "Economie e Finanze" a valere sul capitolo E9305990501, assegnato al Dipartimento Organizzazione e Risorse Umane, il quale assumerà i correlati impegni, nella parte spesa di bilancio, sui fondi destinati alle medesime finalità, rispettivamente, per il pagamento di retribuzioni in denaro, oneri previdenziali a carico dell'Ente e IRAP;

DI DARE ATTO che si provvederà alla stipula del contratto di utenza con il concessionario Polo Strategico Nazionale S.p.A.;

DI ACCERTARE E DI IMPEGNARE le somme di cui al quadro economico per le annualità 2025, 2026 e 2027, come da prospetto sotto riportato:

Anno	ENTRATA		SPESA			
			Servizio			
	Importo (€)	Accertamento cap. di entrata E0120210801	Importo con IVA (€)	Impegno cap. di spesa U0421110306	Importo (€)	Impegno – cap. di spesa U0421110306
2025	5.403.078,05	2043/2025	5.315.931,64	3663/2025	28.624,18	3731/2025 (ASP CZ)
					41.092,95	3660/2025 (REG. CALABRIA)
					17.429,28	3666/2025 (GSA)
2026	3.860.248,24	371/2026	3.797.986,17	399/2026	14.944,22	409/2026 (ASP CZ)
					34.865,44	398/2026 (REG.CALABRIA)
					12.452,41	400/2026 (GSA)
2027	2.685.263,08	236/2027	2.641.952,38	217/2027	10.392,96	225/2027 (ASP CZ)
					24.255,60	216/2027(REG.CALABRIA)
					8.662,14	218/2027 (GSA)
TOTALE	11.948.589,37		11.755.870,19		192.719,18	

DI DEMANDARE al Responsabile di Progetto ogni adempimento successivo alla attuazione del presente provvedimento;

DI NOTIFICARE, a cura del responsabile unico di progetto il presente provvedimento ai soggetti interessati;

DI PROVVEDERE alla pubblicazione integrale del provvedimento sul BURC ai sensi della legge regionale 6 aprile 2011, n. 11 e nel rispetto del Regolamento UE 2016/679 nonché in formato aperto sul sito istituzionale della Regione Calabria, ai sensi della L.R. n. 11 del 06.04.2011, ai sensi del d.lgs.14 marzo 2013, n.33 e nel rispetto del Regolamento UE 2016/679;

DI PROVVEDERE agli obblighi di pubblicazione previsti dall'art.23 del d.lgs. 33/2013 e alle ulteriori pubblicazioni previste dal Piano Triennale di prevenzione della corruzione ai sensi dell'art. 7-bis, comma 3, del d.lgs. 33/2013 e nel rispetto del Regolamento UE 2016/679.

Avverso il presente provvedimento è ammesso ricorso al Tribunale Amministrativo Regionale da proporsi entro il termine di 60 giorni, ovvero ricorso straordinario al Presidente della Repubblica, da proporsi entro 120 giorni.

Sottoscritta dal Responsabile del Procedimento
Aurelio Zaccone
(con firma digitale)

Sottoscritta dal Dirigente Generale
Tommaso Calabrò
(con firma digitale)

REGIONE CALABRIA

REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO ECONOMIA E FINANZE
SETTORE Gestione Entrate

DECRETO DELLA REGIONE

DIPARTIMENTO SALUTE E WELFARE

SETTORE 5 - ASSISTENZA OSPEDALIERA E SISTEMI ALTERNATIVI AL RICOVERO

Numero Registro Dipartimento 392 del 18/03/2025

OGGETTO 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. Affidamento - Accertamenti e Impegni anni 2025 - 2026 - 2027

SI ESPRIME

VISTO di regolarità contabile, in ordine all'entrata, in conformità all'allegato 4/2 del D.lgs. n. 118/2011

Catanzaro 26/03/2025

Sottoscritto dal Dirigente del Settore

Michele Stefanizzi

(con firma digitale)

Cod. Proposta 71431

R E G I O N E C A L A B R I A
REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO ECONOMIA E FINANZE
SETTORE Ragioneria Generale - Gestione Spesa

DECRETO DELLA REGIONE

Numero Registro Dipartimento 392 del 18/03/2025

DIPARTIMENTO SALUTE E WELFARE
SETTORE 5 - ASSISTENZA OSPEDALIERA E SISTEMI ALTERNATIVI AL RICOVERO

OGGETTO 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. Affidamento - Accertamenti e Impegni anni 2025 - 2026 - 2027

SI ESPRIME

VISTO di regolarità contabile, in ordine alla spesa, attestante la copertura finanziaria, in conformità all'allegato 4/2 del D.lgs. n. 118/2011

Catanzaro 26/03/2025

Sottoscritto dal Dirigente del Settore

Umberto Alessio Giordano

(con firma digitale)

Cod. Proposta 71431

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

Regione Calabria

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	18/11/2024

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:	
Cloud Engineering & Migration/PSN Presales PSN Commercial team	Ivana Borrelli 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 Regione Calabria
  - Tommaso Calabrò
  - Email: t.calabro@regione.calabria.it
- Referente Tecnico Regione Calabria
  - Aurelio Zaccone
  - Email: au.zaccone@regione.calabria.it
- Referente di Sicurezza Regione Calabria
  - Aurelio Zaccone
  - Email: au.zaccone@regione.calabria.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 ***Regione Calabria*** di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (ID **2024-0000002205340793-PdF-P8R1**) **opportunamente analizzate e circoscritte alle attività previste dalla Convenzione PSN**.

2 AMBITO

La Regione Calabria, nell'ambito di un percorso di innovazione ed efficienza delle infrastrutture tecnologiche ed informatiche, ha inteso avvalersi della nuova infrastruttura Cloud PSN per disporre di ambienti caratterizzati da maggiore sicurezza, autonomia e alta affidabilità.

I Servizi compresi nel Progetto sono finalizzati ad incentivare il potenziamento e la razionalizzazione delle infrastrutture tecnologiche dell'Amministrazione mediante servizi di Cloud Computing erogati dai Data Center del PSN e strettamente correlati ai desiderata dell'Amministrazione Regionale.

Il presente Progetto si inquadra in tale ambito con la finalità di realizzare, attraverso le soluzioni tecnologiche PSN ed i servizi professionali previsti dalla concessione, un modello funzionale all'innovazione degli stessi processi afferenti all'intero Sistema denominato VALIDA.

VALIDA (VAlutazione LIste Di Attesa) è un Progetto di informatizzazione con cui la Regione ha introdotto e reso note e pervasive le piattaforme abilitanti per la gestione e il controllo delle liste di attesa e per l'analisi proattiva dei dati sanitari, con particolare focus sulla gestione di tutte le fattispecie legate al processo di prenotazione di prestazioni sanitarie.

Con VALIDA è stato istituito il Sovracup Regionale Unico che ha definitivamente sancito un passaggio, da parte dell'Amministrazione, da un modello statico ad un modello di gestione delle prenotazioni di tipo misto, nel senso che conserva l'operatività degli attuali CUP Aziendali (Area Nord, Centro e Sud) ai quali affianca un mainframe denominato per l'appunto il SovraCUP Regionale Unico, che accentra soltanto alcune delle funzionalità attualmente gestite dai CUP Aziendali (essenzialmente, gestione delle agende e delle prenotazioni).

Il SovraCUP Regionale Unico è destinato alla prenotazione di prestazioni sanitarie di specialistica ambulatoriale a carico del Servizio Sanitario Nazionale (SSN) e in libera professione intramoenia, nonché di quelle previste da programmi nazionali e regionali di prevenzione (vaccinazioni, prevenzione serena….), erogate da strutture sanitarie pubbliche, private contrattualizzate e presidi equiparati.

Il modello complessivo proposto si articola su tre livelli logici ed ha consentito nel corso delle ultime due annualità, su infrastruttura a disposizione della Regione Calabria, la realizzazione di un SovraCUP Unico per mezzo del quale sono gestite le agende, formate dalle disponibilità delle risorse che le Aziende mettono a disposizione per i Pazienti e che sono rese prenotabili anche da altre Aziende (agende globali) e dalle agende che le Aziende mantengono per le proprie necessità interne (agende pubbliche e private). La ripartizione tra agende globali, pubbliche e private è decisa, a livello regionale, dal Dipartimento Tutela della Salute e Politiche Sanitarie.

L'insieme dei servizi attualmente erogati fa capo ad un sistema gestionale, realizzato con tecnologia Java e sui canali che espongono le funzionalità all'Utenza finale.

Oltre al sistema gestionale descritto attualmente è possibile erogare i servizi grazie ad un impianto composto da Portale Regionale delle Liste di Attesa e di Prenotazione e APP per il Cittadino, soluzioni per le quali si rende necessaria l'aggregazione, insieme al resto dei servizi dedicati all'Utenza sanitaria, all'interno di un solo ed unico cruscotto ovvero Portale della Sanità Regionale Calabrese.

L'intero sistema correlato al mondo delle prestazioni di specialistica e delle prenotazioni sanitarie, nelle sue componenti funzionali e no, fa affidamento su ambienti a microservizi.

A tale ambiente dovranno essere federate le piattaforme, descritte nel prosieguo, per le quali è previsto Re Platform e/o Re - Architect ai fini del conseguimento degli obiettivi di migrazione da on premise su infrastruttura Cloud PSN oltre che di reingegnerizzazione in ottica Cloud, entro il 30 Giugno 2026, delle componenti di

- accettazione del Prenotato
- istituzione di una Cassa con gestione centralizzata dei relativi processi e flussi di pagamento e ripartimento proventi per i soggetti erogatori mediante istituzione di un Sistema Contabile Unico integrato con PagoPa
- accentramento dei flussi all'interno del cruscotto statistico C / MEF / LP / 730
- integrazione dello stesso CUP con i sistemi LIS, RIS e PS

Le attività previste in termini di servizi e su cui si evidenzia fabbisogno sono, oltre i Servizi Cloud del PSN, le seguenti:

- attività di Assessment strutturata con Analisi e Discovery delle informazioni di maggior dettaglio relativamente ai servizi digitali accennati
- Migrazione e contestuale Re Platform e/o Re - Architect verso il PSN dei workloads di produzione degli applicativi
    1. Sistema CUP e di Gestione Analitico o Cruscotto Sovracup potenziato da modelli di PHM di natura predittiva e funzionale alla classificazione degli utenti per patologia e rischio clinico ovvero alla definitiva istituzione dei percorsi di cura
    2. CUP Unico e relative integrazioni con terzi sistemi presenti presso i Soggetti erogatori
    3. Portale Regionale Liste di Attesa
    4. Portale Sovracup
    5. App Mobile Sovracup
    6. Ecosistema Calabria Sanità
    7. SC-IAM Sanità Calabria - Identity Access Management
- attività V2V, P2V e deploy ex novo degli ambienti serventi di produzione su ambiente PSN idonei ad ospitare gli impianti applicativi menzionati con distinzione dei layer applicativi dal layer dati
- messa in sicurezza, tunings sistemistico e IT Service Operation degli ambienti e dei workload migrati su infrastruttura PSN.

Il piano dell'intervento consentirà di dotare di risorse, tecnologie e sistemi abilitanti il disegno e l'esecuzione di un percorso basato sui principi del Cloud First e Once Only ed in grado di estendere e diffondere l'approccio innovativo per il potenziamento e la messa in sicurezza dei servizi e dei processi dell'amministrazione attualmente basati sullo stack architetturale interamente ospitato on premise.

Di seguito, sono riportati i Servizi dedicati all'utenza che l'Amministrazione intende migrare, opportunamente classificati ed indicati nel PdF ai paragrafi 5.1 e 5.1.5:

Servizi	Classificazione	Tipo di Migrazione
Sistema CUP e Cruscotto di Gestione Analitico	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Population Health Management + Percorsi di cura Analytic Dashboard	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Portale Regionale Liste di Attesa	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Portale Sovracup	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
App Mobile Sovracup	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Ecosistema Calabria Sanità	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
SC-IAM Sanità Calabria – Identity Access Management	Critico	Modalità B - aggiornamento in sicurezza di applicazioni in cloud

L'Amministrazione richiede servizi specialistici ed una fase di Assessment propedeutica alla migrazione dei Servizi indicati con la predisposizione di un piano di attività avente ad oggetto:

- identificazione e analisi organizzativa dei Servizi con la definizione di modalità di accesso e destinatari/utenza;
- individuazione delle componenti on premise sostituibili con servizi cloud-native;
- stack tecnologico in uso con individuazione di eventuali criticità e vulnerabilità e dei livelli di rischio legati al mancato rispetto dei principi di sicurezza e di accessibilità;
- censimento e la necessità di potenziare e integrare le misure di sicurezza adottate in materia di Endpoint Protection Platform;
- censimento delle policy di sicurezza sui dati;
- identificazione Stakeholders, analisi degli obiettivi di breve periodo e pianificazione per il Go Live dei Servizi;
- analisi e verifica dell'integrazione dei suddetti servizi con sistemi di pagamento elettronici;
- l'individuazione di vincoli normativi e tecnologici.

La modalità di migrazione dei sette Servizi sul Cloud del PSN è la B che prevede l'*Aggiornamento in sicurezza di Applicazioni in Cloud* con l'adozione di una strategia che ha l'obiettivo di ripensare significativamente l'architettura in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare appieno i servizi cloud-native offerti dal Cloud Service Provider per massimizzare i benefici che ne derivano.

La Classificazione del Dato dei Servizi comunicata da ACN all'Amministrazione, trascritta nel PdF inviato al PSN, è Critico.

In ottemperanza a quanto espresso dall'Amministrazione e in coerenza con gli approfondimenti tecnici congiunti effettuati in fase di definizione del presente Progetto, la soluzione proposta, per rispondere alle esigenze dell'Amministrazione nell'ambito dei servizi PSN, prevede:

- *Analisi* e *Discovery* dei requisiti tecnici e funzionali dei sette Servizi indicati nel PdF comprendenti
    - la piattaforma oggetto della migrazione
    - le Applicazioni a supporto dei Servizi
    - i Dati oggetto di migrazione
    - i Livello di Servizio dei Servizi
    - eventuali finestre utili per la migrazione

    - eventuali periodi di indisponibilità dei Servizi
    - Cloud Maturity Model
    - analisi della sicurezza dell'ambiente da migrare
- disponibilità di infrastrutture Cloud sul PSN adeguatamente dimensionate quali,
    - Public Cloud PSN Managed
- supporto all'Amministrazione per le fasi di
    - *Set up*, comprendente
        - predisposizione dell'infrastruttura target nel DC del PSN
        - disegno dei workload
        - definizione architettura logica
        - configurazione ambienti
    - *Migrazione* dei Servizi
        - trasferimento dei dati
        - implementazione policy di sicurezza
        - impostazione del monitoraggio
    - *Collaudo* finalizzato a testare le procedure e modalità della migrazione
- Security Services Professional
- IT Infrastructure Service Operations

Si precisa che

- nel Progetto non è prevista la fornitura di alcuno Software (intese Licenze d'uso commerciali e/o gratuite) a completamento dei nuovi ambienti Cloud sul PSN,
- eventuali Licenze ovvero Applicazioni non compresi nel Configuratore saranno forniti dalla PA e non da PSN.

Sulle Licenze di Sistemi Operativi e Middleware di proprietà che l'Amministrazione intende importare sui suddetti ambienti (modalità Bring Your own License, BYOL) devono essere attive le fee software e assurance e le versioni devono avere un path di update (active e security update) che copre l'intero periodo contrattuale.

La modalità di erogazione del Servizi implica l'impiego di Internet. Il DC del PSN è collegato a Internet per consentire all'Amministrazione di usufruire dei Servizi Cloud Computing senza soluzione di continuità ed ai propri Fornitori di accedere da remoto.

Il presente Progetto non rientra nell'ambito dei finanziamenti PNRR.

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"
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

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato D)	Schema di Contratto di Utenza
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato H)	Indicatori di Qualità
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato I)	Flussi informativi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato L)	Elenco dei Servizi Core, no Core e CSP

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

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

Tabella 7: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
CMP	Cloud Management Platform
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
HA	High Availability
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PSN	Polo Strategico Nazionale
VM	Virtual Machine

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	Oracle Cloud
Servizi di Migrazione	
Servizi Professionali	Re-Architect
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

Tabella 9: Servizi Proposti

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

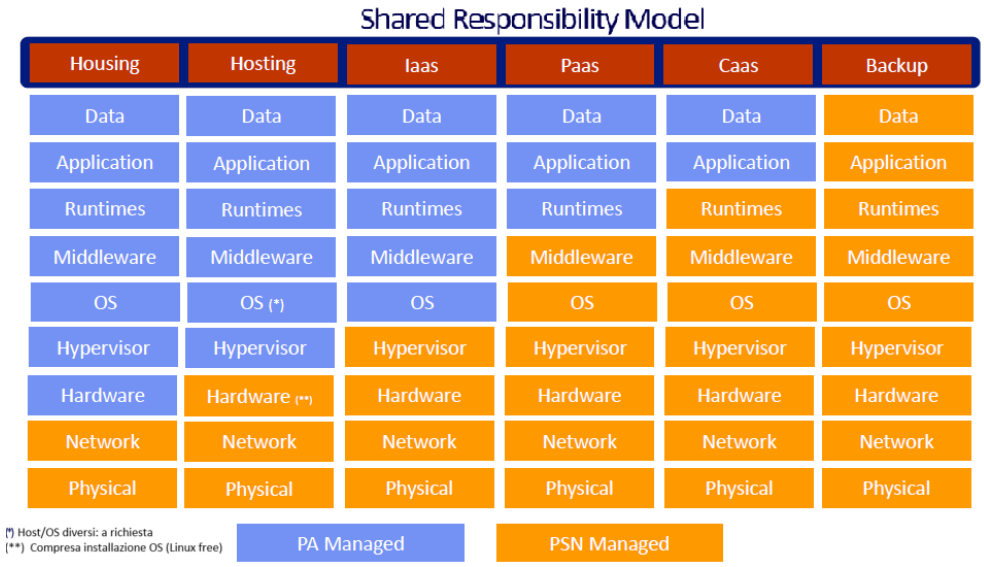

Figura 1 Shared Responsibility Model

L'Amministrazione, così come indicato al precedente Capitolo 2, ha comunicato nel PdF la Classificazione dei Dati del Servizio da migrare sul Cloud del PSN – trasmessa dall'Agenzia per la Cybersicurezza Nazionale (ACN).

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/

5.2 PUBLIC CLOUD PSN MANAGED

5.2.1 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**.

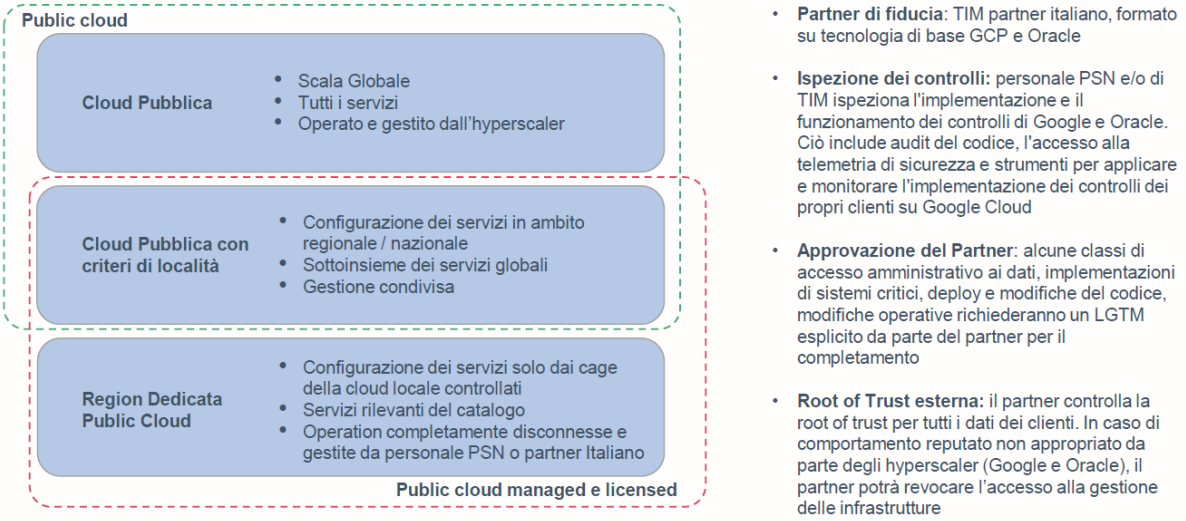

Figura 2 Public Cloud vs Public Cloud Managed

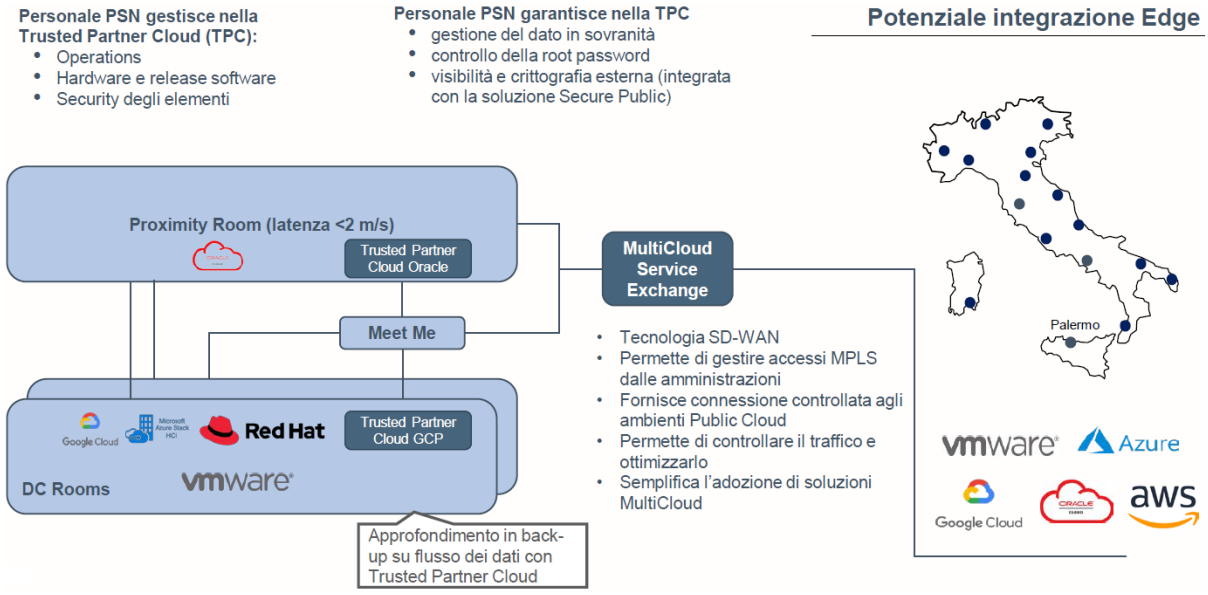

Figura 3 Architettura Public Cloud Managed

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 (Continouos deployment) per rilasciare fix, nuove features o rimedi ad esposizioni di sicurezza: uno dei vantaggi del Public Cloud PSN Managed consiste proprio nel poter sfruttare questi benefici (soprattutto la celerità nel rimediare a potenziali esposizioni di sicurezza). Allo stesso tempo però l'MSP-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

5.2.2 Personalizzazione del servizio

Il Servizio Public Cloud PSN Managed individuato e proposto all'Amministrazione è Oracle Cloud, una potente piattaforma che offre una importante gamma di funzionalità per supportare la Suddetta nel proprio percorso verso la digitalizzazione. Essendo una piattaforma cloud, le sue capacità sono accessibili attraverso Internet, consentendo all'Amministrazione di accedere e utilizzare risorse informatiche, come server, storage e servizi software, in modo flessibile.

Tra le sue capacità principali, spicca la versatilità nell'eventuale evoluzione contrattuale delle risorse informatiche necessarie.

La sicurezza è una priorità fondamentale, con misure avanzate di protezione dei dati e delle applicazioni.

La flessibilità è un'altra caratteristica chiave di Oracle Cloud Infrastructure, che supporta una varietà di carichi di lavoro, dalle istanze di calcolo alle soluzioni di storage e database. Grazie alla sua architettura è in grado di integrarsi facilmente con le tecnologie esistenti e di supportare l'adozione di nuove soluzioni.

La piattaforma è dotata di strumenti di monitoraggio e gestione avanzati, che consentono di monitorare le prestazioni ed ottimizzare l'utilizzo delle risorse in tempo reale.

Ogni componente costituente Oracle Cloud è stata ingegnerizzata con elementi peculiari di alta affidabilità e resilienza, quali:

- Virtual Network, le componenti di network sono ridondate intra-region
- Compute, anti-affinity & HA tramite fault domains
- Storage, (live migration & relocation disponibile). Lo storage è replicato sui fault domains
- Database Node, HA (Active/Active) tramite RAC
- DC Power & Connectivity, i DC di PSN sono Tier 4 e garantiscono massimo livello di protezione per fault di network e power
- Maintenance, la maintenance ordinaria è eseguita in modalit~ rolling senza downtime

Il servizio PSN Managed Oracle Cloud aiuta ad affrontare la sovranità digitale con le seguenti caratteristiche:

- separazione fisica e/o logica dei workloads e dei rispettivi dati (Sovranità dei dati)
- ispezionabilità per garantire i controlli di conformità (Trasparenza sui dati)
- residenza dei dati e workload in EU/Italia (Residenza dei dati)
- supporto locale con personale del PSN

Gli elementi costituenti il Servizio Public Cloud PSN Managed Oracle Cloud sono i seguenti:

- Compute VM, un ambiente di computazione virtuale multi tenant scalabile nel quale eseguire le applicazioni con prestazioni, controllo e resilienza built-it
- Base Database Service - Virtual Machine, esegue workload Oracle Database Enterprise Edition e Standard Edition su Virtual Machine (VM) flexible. Supporta ii RAC.
- GoldenGate, lo strumento di replica per i database Oracle, utilizzato per l'integrazione dei dati, l'alta disponibilità e le migrazioni online.
- Storage Volumi a blocchi Standard e Performance, offre Storage a blocchi affidabile e ad altre

prestazioni progettato per funzionare con una gamma di VM ed istanze Bare Metal. Con la ridondanza built-in, i volumi a blocchi risultano persistenti e durevoli oltre la durata e possono essere ridimensionati fino a 1 PB per istanza di computazione

- Storage ad Oggetti consente di memorizzare qualsiasi tipo di dati nel formato nativo. È ideale per applicazioni moderne che richiedono scalabilità e flessibilità, poiché può essere utilizzato per consolidare più origini dati per scopi di analisi, backup ovvero archiviazione
- FastConnect, opzione di connettività di rete dedicata, privata e sicura per la connessione della Sede dell'Amministrazione on premise ad Oracle Cloud

La Landing Zone (LZ) OCI include vari servizi di sicurezza preconfigurati che possono essere implementati in tandem con l'architettura generale per una solida postura della sicurezza.

I Servizi compresi nella LZ OCI sono i seguenti:

- Security
    - Observability, Logging Analytics e Monitoring
    - Key Management, OCI - External Key Management
    - Application Firewall, Web Application Firewall e Network Firewall
- Application, Streaming

Il Public Cloud PSN Managed Oracle Cloud è stato definito sulla base delle risorse necessarie per garantire efficienza dei sette Servizi da migrare sul Cloud e configurato sulla base delle risorse necessarie per garantire adeguate prestazioni dei domini applicativi.

Il Progetto comprende anche l'attivazione del Backup compiuto con strumento native Oracle e memorizzato su Object storage.

Il Backup garantirà il salvataggio di una copia dei Dati consolidati sui Servizi Public Cloud PSN Managed OCI per consentire il recupero in un momento successivo. Il servizio di Backup permetterà di salvare periodicamente i Dati in modo da proteggerli da eventuali attacchi informatici ovvero da modifiche e/o cancellazioni involontarie.

La quota storage necessaria al Backup è stata calcolata sul fabbisogno complessivo dello Storage Compute (21,5 TB) e DB (23,5 TB), valutando le seguenti policy:

- numero full Mese, 2
- numero incrementale Mese (giorni), 18
- tasso variazione annuo stimato Dati (%), 5

Lo spazio di archiviazione complessivo riservato al Backup, assunti la totalità di dati sorgente definita nel Progetto, è stimato in circa 200 TB compresi 17 TB Object Storage necessari all'Amministrazione per Data Laking.

La modalità di erogazione del Servizi, come predetto, implica l'impiego di Internet.

La configurazione del Public Cloud Managed Oracle Cloud comprende anche le FastConnect perché sarà definita una connessione privata e sicura tra la Cittadella Regionale ed Oracle Cloud esclusivamente per il periodo di migrazione delle Applicazioni e Database stimata in circa 45 giorni.

A livello di Fabbrica saranno configurati un router linking e policy tra la VRF privata di OCI e la VRF del Tenant di connettività dedicata di altro OLO, prevista in un altro Contratto di Utenza già sottoscritto tra l'Amministrazione ed il PSN, per consentire l'interoperatività tra il Tenant OCI e l'on premise dell'Amministrazione.

In riferimento Base Database Service - Virtual Machine si precisa ed evidenzia che la modalità di Licensing del Servizio Base Database Service - Virtual Machine è BYOL (Bring Your Own License). Ai fini dell'erogazione delle PaaSDB Oracle è vincolante che l'Amministrazione abbia la disponibilità delle Licenze Enterprise Edition nella versione Unlimited Socket, ultima o penultima versione dichiarata da Oracle, comprensive del RAC e degli altri prodotti software idonei e completi degli strumenti a supporto del Servizio Oracle DB.

L'Amministrazione, in merito ai Sistemi Operativi ed allo stack middleware, deve impegnarsi ad aggiornare costantemente le versioni in coerenza con gli standard richiesti dal PSN per tutta la durata del Contratto e valutarne, eventualmente e tempestivamente, la sostituzione con altre distribuzioni valide.

Il PSN non garantisce la certificazione e il funzionamento di Sistemi Operativi obsoleti nella propria infrastruttura e non sarà ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17).

I tool di monitoraggio e diagnostica sono a carico dell'Amministrazione.

Nelli seguenti tabelle è dettagliata la consistenza delle VM costituenti i sette Servizi indicati nel PdF e le risorse computazionali ad essi attribuite.

Sistema CUP e Cruscotto di Gestione Analitico

Ambiente	Hostname	vCPU	RAM	Storage	Storage Data	OS	Note
Pre-Prod	cvalida-lx-lbc01	2	4	50		RHEL 8.x	
Pre-Prod	cvalida-lx-appl01	4	48	100		RHEL 8.x	
Pre-Prod	cvalida-lx-appl02	4	48	100		RHEL 8.x	
Pre-Prod	ENG-VALIDA-DB-PreProd	8	32	300	4.000		Base DB Server Oracle BYOL
DWH	dvalida-lx-lbc01	2	4	50		RHEL 8.x	
DWH	dvalida-lx-appl01	8	32	100		RHEL 8.x	
DWH	dvalida-lx-appl02	8	32	100		RHEL 8.x	
DWH	ENG-VALIDA-DB-DWH	16	32	300	4.000		Base DB Server Oracle BYOL
Test	tvalida-lx-lbc01	2	4	50		RHEL 8.x	
Test	tvalida-lx-appl01	4	32	100		RHEL 8.x	
Test	tvalida-lx-appl02	4	32	100		RHEL 8.x	
Test	tvalida-lx-appl03	4	32	100		RHEL 8.x	

Test	tvalida-lx-WSO2-EII	8	16	100		RHEL 8.x	
Test	tvalida-lx-WSO2-DAS	4	16	100		RHEL 8.x	
Test	ENG-VALIDA-DB-Test	8	32	300	4.000		Base DB Server Oracle BYOL
Produzione	pvalida-lx-lbc01	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc02	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc03	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-lbc04	2	4	50		RHEL 8.x	
Produzione	pvalida-lx-appl01	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl02	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl03	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl04	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl05	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl06	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl07	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl08	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl09	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl10	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl11	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl12	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl13	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl14	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl15	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl16	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl17	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-appl18	8	64	100		RHEL 8.x	
Produzione	pvalida-lx-WSO2-EII-1	8	32	200		RHEL 8.x	
Produzione	pvalida-lx-WSO2-EII-2	8	32	200		RHEL 8.x	
Produzione	pvalida-lx-WSO2-DAS	12	32	1.024		RHEL 8.x	
Produzione	pvalida-lx-zabbix	8	16	400		RHEL 8.x	
Produzione	ENG-VALIDA-DB-Prod1	48	128	300	4.000		Base DB Server Oracle BYOL
Produzione	ENG-VALIDA-DB-Prod2	48	128	300			Base DB Server Oracle BYOL
		370	**1932**	**6374**	**16000**		

Tabella 10: Dettaglio fabbisogno PSN Sistema CUP e Cruscotto di Gestione Analitico

Population Health Management + Percorsi di cura Analytic Dashboard

Ambiente	Hostname	vCPU	RAM	Storage	Storage Object	OS
Produzione	Management_PHM	8	16	250		Oracle Linux 8.x
Collaudo	Management_PHM	4	8	100		Oracle Linux 8.x
Produzione	Storage Object - Data Laking				15000	Oracle Linux 8.x
		12	**24**	**350**	**15000**	

Tabella 11: Dettaglio fabbisogno PSN Population Health Management + Percorsi di cura Analytic Dashboard

App Mobile Sovracup, Portale Sovracup, Portale Regionale Liste di Attesa

Ambiente	Hostname	vCPU	RAM	Storage	Storage Data	OS	Note
Produzione	Application Wrk1	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk2	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk3	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk4	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk5	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk6	8	16	50		Oracle Linux 8.x	
Produzione	Application CntrlPln1	8	16	50		Oracle Linux 8.x	
Produzione	Application CntrlPln2	8	16	50		Oracle Linux 8.x	
Produzione	Application CntrlPln3	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk1	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk2	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk3	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk4	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk5	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk6	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk7	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk8	8	16	50		Oracle Linux 8.x	
Produzione	Application Wrk9	8	16	50		Oracle Linux 8.x	
Produzione	HA Pro1	4	8	25		Oracle Linux 8.x	
Produzione	HA Pro2	4	8	25		Oracle Linux 8.x	
Produzione	Registry	8	16	250		Oracle Linux 8.x	
Produzione	GrayLog	4	8	250		Oracle Linux 8.x	
Produzione	NFS	4	8	250		Oracle Linux 8.x	
Produzione	NFS	4	8	250		Oracle Linux 8.x	
Produzione	NFS	4	8	250		Oracle Linux 8.x	
Collaudo	Application Wrk1	8	16	50		Oracle Linux 8.x	
Collaudo	Application Wrk2	8	16	50		Oracle Linux 8.x	
Collaudo	Application Wrk3	8	16	50		Oracle Linux 8.x	
Collaudo	Application CntrlPln1	8	16	50		Oracle Linux 8.x	
Collaudo	Application CntrlPln2	8	16	50		Oracle Linux 8.x	
Collaudo	Application CntrlPln3	8	16	50		Oracle Linux 8.x	

Collaudo	NFS	4	8	250		Oracle Linux 8.x	
Collaudo	DBPortaleUnico/App/PHM	8	32	125	500		Base DB Server Oracle BYOL
Produzione	DBPortaleUnico/App/PHM	32	128	250	1500		Base DB Server Oracle BYOL
		268	**616**	**3125**	**2000**		

Tabella 12: Dettaglio fabbisogno PSN App Mobile Sovracup, Portale Sovracup, Portale Regionale Liste di Attesa

Ecosistema Calabria Sanità

Ambiente	Hostname	vCPU	RAM	Storage	Storage Data	OS	Note
Collaudo/Pre-Prod	COL_WEBSERV-ECOSANITA-REGCAL	8	16		500	Oracle Linux 8.x	
Collaudo/Pre-Prod	COL_DB	8	32		270	Oracle Linux 8.x	Base DB Server Oracle BYOL
Collaudo/Pre-Prod	COL-VOCAL	4	8	100		Oracle Linux 8.x	
Collaudo/Pre-Prod	Security2	4	4		50	Oracle Linux 8.x	
Produzione	PRO_WEBSERV-ECOSANITA-REGCAL	8	8		1.000	Oracle Linux 8.x	
Produzione	WindowsTec	8	16		200	Win Server 2019 Std	
Produzione	PRO_DB	16	64		512	Oracle Linux 8.x	Base DB Server Oracle BYOL
Produzione	Security	8	16	100	2.000	Oracle Linux 8.x	
Produzione	PRO-VOCAL	8	16	250	1.000	Oracle Linux 8.x	
Produzione	PHP8-PRO_WEBSERV-ECOSANITA-REGCAL	16	32		1.000	Oracle Linux 8.x	
Produzione	Security	16	32	250	250	Oracle Linux 8.x	
Produzione	Security	16	32	250	250	Oracle Linux 8.x	
		120	**276**	**950**	**7032**		

Tabella 13: Dettaglio fabbisogno PSN Ecosistema Calabria Sanità

SC-IAM Sanità Calabria – Identity Access Management

Ambiente	Hostname	vCPU	RAM	Storage	Storage Data	OS
Produzione	API _Prod	24	64	250	3.000	Oracle Linux 8.x
Collaudo	API_Coll	8	16	125	500	Oracle Linux 8.x
		32	**80**	**375**	**3500**	

Tabella 14: Dettaglio fabbisogno PSN SC-IAM Sanità Calabria – Identity Access Management

Di seguito, la configurazione del Servizio Public Cloud Managed Oracle suddiviso in base alle distinte tipologie, comprendente anche le risorse correlate all'ambito Secure Device e aggiuntive, quest'ultime utili a gestire gli ampliamenti delle VM, determinata dall'analisi tecnica compiuta con l'Amministrazione e funzionale alla migrazione dei suddetti Servizi:

Servizio	Tipologia	Service Element / Unit	Q.tà
Public Cloud PSN Managed Oracle Cloud	OCI - Compute - Standard - E5 - OCPU	OCPU Per Hour	335
	OCI - Compute - Standard - E5 - Memory	Gigabyte Per Hour	2.555
	OCI - Block Volume Storage	Gigabyte Storage Capacity Per Month	55.180
	OCI - Block Volume Performance	Performance Units Per Gigabyte Per Month	888.600
	OCI - Object Storage - Requests	10,000 Requests per Month (first 50,000 free)	200
	OCI - Object Storage - Storage	Gigabyte Storage Capacity Per Month	200.000
	OCI - FastConnect 1 Gbps	Port Hour	2
	OCI - Oracle Base Database Service - BYOL	OCPU Per Hour	105
	OCI - GoldenGate	OCPU Per Hour	10
	OCI - Web Application Firewall - Instance	Instance Per Month	1
	OCI - Web Application Firewall - Requests	1,000,000 Incoming Requests Per Month	50
	OCI - Network Firewall - Instance	Instance Per Hour	1
	OCI - Network Firewall - Data Processing	Gigabyte (GB) of Data Processed	4.096
	OCI - Logging - Storage	Gigabyte Log Storage Per Month	100
	OCI - Logging Analytics - Active Storage	Logging Analytics Storage Unit Per Month	10
	OCI - Logging Analytics - Archival Storage	Logging Analytics Storage Unit Per Hour	5
Industry Standard	Housing	IP Pubblici /29 (8 indirizzi)	2
	Sistemi Operativi	Windows Server STD CORE (2 core)	4

Tabella 15: Dettaglio consistenza Servizi Public Cloud PSN Managed Oracle Cloud & Industry Standard

Il Servizio OCI GoldenGate si intende valido per 10 OCPU ed attivo per numero 45 giorni di utilizzo.

5.2.3 Dettaglio Infrastruttura da migrare

Nella seguente tabella è indicata la parziale configurazione dei Servizi che l'Amministrazione intende migrare sul Cloud del PSN.

L'elenco acquisito delle VM indicate potrebbe variare in seguito alle attività di Analisi e Discovery che saranno compiute dopo la stipula del Contratto con il PSN, durante la quale sarà determina la consistenza attuale degli altri Servizi per i quali è prevista la migrazione sul Cloud del PSN.

Servizio	Ambiente	Hostname	vCPU	RAM	OS Storage	Data Storaage	OS
Sistema Gestione Analitico Sovracup	Collaudo/Pre-Produzione	cvalida-lx-lbc01	2	4	50		RHEL 8.x
	Collaudo/Pre-Produzione	cvalida-lx-appl01	4	8	100		RHEL 8.x
	Collaudo/Pre-Produzione	cvalida-lx-appl02	4	8	100		RHEL 8.x
	Collaudo/Pre-Produzione	ENG-VALIDA-LBC1-COLL	2	4	50		RHEL 8.x
	Collaudo/Pre-Produzione	ENG-VALIDA-DB-COLL	8	32	300	4096	RHEL 8.x
	Collaudo/Pre-Produzione	ENG-VALIDA-APPL1-COLL	4	32	100		RHEL 8.x
	Collaudo/Pre-Produzione	ENG-VALIDA-APPL2-COLL	4	32	100		RHEL 8.x
	Produzione	pvalida-lx-lbc01	2	4	50		RHEL 8.x
	Produzione	pvalida-lx-lbc02	2	4	50		RHEL 8.x
	Produzione	pvalida-lx-lbc03	2	4	50		RHEL 8.x
	Produzione	pvalida-lx-lbc04	2	4	50		RHEL 8.x
	Produzione	pvalida-lx-appl01	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl02	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl03	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl04	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl05	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl06	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl07	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl08	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl09	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl10	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl11	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl12	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl13	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl14	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl15	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl16	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-appl17	8	48	100		RHEL 8.x
	Produzione	pvalida-lx-zabbix	8	16	400		RHEL 8.x
	Produzione	pvalida-lx-oracledb	48	64	110	2500	RHEL 8.x
	Collaudo/Pre-Produzione	cvalida-lx-master	4	8	50	-	Oracle Linux 8.7
	Collaudo/Pre-Produzione	cvalida-lx-node1	4	8	50	-	Oracle Linux 8.7
	Collaudo/Pre-Produzione	cvalida-lx-node2	4	8	50	-	Oracle Linux 8.7
	Collaudo/Pre-Produzione	cvalida-lx-node3	4	8	50	-	Oracle Linux 8.7

	Collaudo/Pre-Produzione	cvalida-lx-nfs	4	8	50	100	Oracle Linux 8.7
	Collaudo/Pre-Produzione	cvalida-lx-registry	4	4	40	50	Oracle Linux 8.7
	Collaudo/Pre-Produzione	cvalida-lx-proxy	4	4	40	-	Oracle Linux 8.7
	Produzione	pvalida-lx-master1	16	32	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-master2	16	32	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-master3	16	32	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node1	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node2	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node3	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node4	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node5	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-node6	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-nfs	4	8	50	500	Oracle Linux 8.7
	Produzione	pvalida-lx-proxy1	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-proxy2	8	16	50	-	Oracle Linux 8.7
	Produzione	pvalida-lx-azzerowpress	4	8	50	250	Oracle Linux 8.7
Ecosistema Calabria Sanità	Collaudo/Pre-Produzione	COL_WEBSERV-ECOSANITA-REGCAL	8	16		500	Centos 7.x
	Collaudo/Pre-Produzione	COL_DB	5	8		270	Centos 7.x
	Collaudo/Pre-Produzione	COL-VOCAL	4	8	100		DEBIAN 9
	Collaudo/Pre-Produzione	Security2	4	4		20	PFSense 2.x
	Produzione	PRO_WEBSERV-ECOSANITA-REGCAL	2	2		1000	Centos 7.X
	Produzione	WindowsTec	4	8		200	Win Server 2016
	Produzione	PRO_DB	15	16		520	Centos 7.x
	Produzione	Security	8	12	100	2000	Centos 7.x
	Produzione	PRO-VOCAL	4	8	125	200	DEBIAN 9
	Produzione	PHP8-PRO_WEBSERV-ECOSANITA-REGCAL	8	16		1000	Centos 7.x

Tabella 16: Dettaglio consistenza AS IS

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

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

5.2.5 Specifiche di collaudo

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

5.3 CONSOLE UNICA

La Fornitura prevede l'erogazione alle PAC, in maniera continuativa e sistematica, di una serie di servizi afferenti ad un Catalogo predefinito e gestito attraverso una Console Unica dedicata.

Il PSN metterà a disposizione delle Amministrazioni Contraenti una piattaforma di gestione degli ambienti cloud unica (CU) personalizzata, interoperabile attraverso API programmabili che rappresenterà per la PA l'interfaccia unica di accesso a tutte le risorse acquistate nell'ambito della convenzione. In particolare, la CU garantirà la possibilità alle Amministrazioni di configurare ed istanziare, in autonomia e con tempestività, le risorse contrattualizzate per ciascuna categoria di servizio e, accedendo alle specifiche funzionalità della console potrà gestire, monitorare ed utilizzare i servizi acquisiti.

Infine, attraverso la CU, l'Amministrazione avrà la possibilità di segnalare anomalie sui servizi contrattualizzati tramite l'apertura guidata di un ticket per la cui risoluzione il PSN si avvarrà del supporto di secondo livello di specialisti di prodotto/tecnologia.

5.3.1 Overview delle caratteristiche funzionali

La CU è progettata per interagire col PSN CLOUD ed integrare le funzionalità delle console native di cloud management degli OTT, fornendo un'interfaccia unica in grado di guidare in modo semplice l'utente nella definizione e gestione dei servizi sottoscritti utilizzando anche la tassonomia e le modalità di erogazione dei servizi previsti nella convenzione. Tale piattaforma presenta un'interfaccia applicativa responsive e multidevice ed è utilizzabile, oltre che in modalità desktop, anche mediante dispositivi mobili Android o iOS e abilita i sottoscrittori ad accedere in maniera semplificata agli strumenti che consentono di: √gestire in modalità integrata i profili di accesso alla CU tramite le funzionalità di Identity Management; disegnare l'architettura dei servizi acquistati e gestirne le eventuali variazioni; √consentire l'interfacciamento attraverso le API per la gestione delle risorse istanziate ma anche per definire un modello di IaC (Infrastructure as Code); segnalare eventuali anomalie in modalità "self".

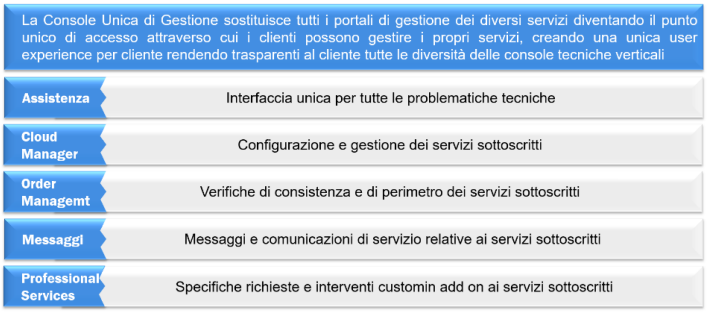

Figura 4 Funzionalità CU

Le aree di interazione che la piattaforma CU consente di gestire sono:

1. Area Attivazione contrattuale. All'atto dell'adesione alla convenzione da parte dell'Amministrazione, sulla CU: √saranno caricati i dati contrattuali ed anagrafici dell'Amministrazione; √generato il profilo del referente Master (Admin) della PA a cui sarà inviata una "Welcome Letter" con il link della piattaforma, l'utenza e la password (da modificare al primo login) per l'accesso alla CU; √sarà configurato il tenant dedicato alla PA, che rappresenta l'ambiente cloud tramite il quale la PA usufruirà dei servizi acquisiti (IaaS, PaaS, ecc.).

2. Area Access Management e profilazione utenze. L'accesso alla CU è gestito totalmente dal sistema di Identity Access Management (IAM). Gli utenti, previa registrazione, saranno censiti nello IAM, e con le credenziali rilasciate potranno accedere dalla console alle risorse allocate all'interno del proprio tenant. Anche la creazione dei profili delle utenze e la loro associazione

con gli account degli utenti sarà gestita tramite le funzionalità di IAM in un'apposita sezione della CU denominata "Gestione Utenze".

3. Area Design & Delivery. Attraverso tale modulo della CU, l'Amministrazione Contraente potrà configurare in autonomia i servizi acquistati secondo le metriche definite per la convenzione, costruendo, anche mediante l'utilizzo di un tool di visualizzazione, la propria architettura cloud sulla base delle risorse contrattualizzate. Successivamente la CU, interagendo in tempo reale attraverso le API dei servizi cloud verticali, consentirà l'immediata attivazione delle risorse e dei servizi previsti nell'architettura attraverso la creazione di uno o più tenant logici per segregare le risorse computazionali dei clienti (Project). Il processo è gestito mediante un workflow automatizzato di delivery implementato tramite l'uso di Blueprint. La CU esporrà anche delle API affinché la singola Amministrazione Contraente possa interagire attraverso i propri tools di CD/CI, IaC (Terraform, Ansible…) oppure attraverso una propria CU come ulteriore livello di astrazione e indipendenza (qualora ne avesse già a disposizione e quindi creare una CU Master Controller che interagisce con quella del PSN appunto via API).
4. Area Management & Monitoring. La piattaforma consentirà ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali. Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.
5. Area Self Ticketing. Consente alla PA di segnalare in modalità self le anomalie riscontrate sui servizi cloud contrattualizzati.

5.3.2 Modalità di accesso

L'accesso in modalità sicura alla Console Unica prevede l'utilizzo del sistema di Identity Management, il cui form di login è integrato nell'interfaccia web. Tale sistema gestisce le identità degli utenti registrati e consente sia l'accesso in modalità desktop, sia tramite dispositivi mobili Android o iOS. Gli utenti, autorizzati dal sistema di Identity Access Management, potranno accedere dalla console alle risorse allocate all'interno del proprio tenant, sia per attività di "Design & Delivery" sia per attività di "Management & Monitoring".

5.3.3 Interfaccia applicativa della Console Unica

La Console Unica espone un'interfaccia profilata per ciascuna Amministrazione Contraente, presentando il set di servizi contrattualizzati e abilitandola ad eseguire le operazioni desiderate in piena autonomia. Di seguito è riportata una breve descrizione delle sezioni della Console Unica che sono rese disponibili.

Dall'Home Page è possibile accedere alle sezioni:

- Dashboard: consente di visualizzare il riepilogo dei dati contrattuali, verificare lo stato dei propri servizi IaaS, PaaS, ecc, il tracking dei ticket aperti e lo storico delle operazioni effettuate. In particolare, come evidenziato in Figura 4, cliccando sul widget di una specifica categoria di servizio (ad esempio Compute), sarà possibile visualizzare direttamente, secondo le metriche della convenzione, il dettaglio delle quantità totali delle risorse acquistate, quelle già utilizzate e le quantità ancora disponibili. Inoltre, accedendo al menu del profilo presente nell'header dell'interfaccia della Console Unica, il referente dell'Amministrazione avrà la possibilità di impostare gli indirizzi e-mail a cui inviare tutte le notifiche previste nella sezione Messaggi e selezionare altre impostazioni di base (lingua, ecc.).

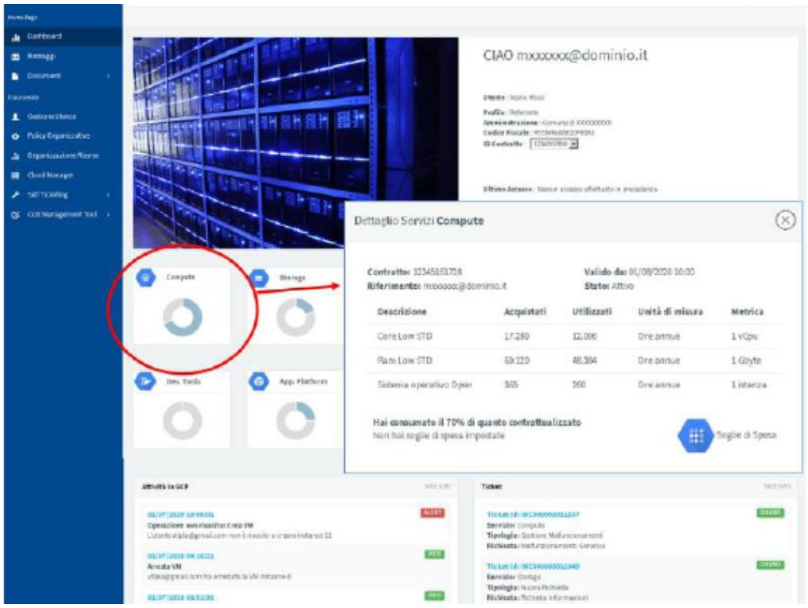

Figura 5 Dashboard CU

- Cloud Manager: in questa sezione, per tutti i servizi della convenzione, ciascuna Amministrazione potrà, nell'ambito della funzione di Design & Delivery:
  - costruire l'architettura cloud di ciascun Project all'interno del proprio tenant;
  - attivare i servizi in self-provisioning;
  - nell'ambito della funzione di Management & Monitoring:
  - effettuare operazioni di scale up e scale down sui servizi contrattualizzati;
  - gestire e monitorare tali servizi accedendo direttamente all'opportuna sezione della console.

Dettagliando ulteriormente la sezione di Design & Delivery, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di definire e configurare le risorse cloud contrattualizzate in modalità semplificata ed aderente ai requisiti e alla classificazione dei servizi della Convenzione, garantendo massima autonomia e tempestività nell'attivazione.

Il referente dell'Amministrazione, accedendo dalla sezione "I tuoi servizi" alla dashboard del Cloud Manager potrà nella fase di Design & Delivery:

- selezionare, utilizzando l'apposito menu a tendina presente nell'header della pagina, un Project tra quelli esistenti;
- visualizzare sia le categorie di servizio in cui sono state attivate risorse con il relativo dettaglio (identificativo della risorsa) sia quelle che non hanno risorse istanziate;
- istanziare in modo semplificato, per ciascuna categoria di servizi della Convenzione, attraverso la funzionalità "Configura", nuove risorse cloud utilizzando una procedura guidata che espone solo le funzionalità base per l'attivazione delle risorse cloud garantendo velocità di esecuzione. Nel caso in cui l'Amministrazione voglia, invece, utilizzare tutte le funzionalità di configurazione del Cloud

Manager potrà accedervi direttamente dal tasto “Funzionalità Avanzate” presente in ciascuna finestra di configurazione.

- monitorare, in fase di attivazione delle risorse, lo stato di avanzamento dei consumi per la specifica categoria di servizi nel Project selezionato in modo da avere sempre a disposizione una vista delle quantità disponibili e in uso.

Dettagliando ulteriormente la sezione di Management & Monitoring, dopo aver terminato la fase di attivazione delle risorse cloud all’interno del Project selezionato, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di:

- gestire la singola risorsa accedendo direttamente alle specifiche funzionalità presenti console tramite il button “Gestisci”;
- monitorare le performance della risorsa accedendo alle funzionalità di monitoraggio tramite il relativo button “Monitora”.

In alternativa, il referente dell’Amministrazione ha la possibilità di accedere alle funzionalità avanzate della dashboard tramite il relativo button “presente nell’header della sezione.

5.4 Servizi e Piano di Migrazione

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assessment effettuati in fase di definizione delle esigenze dell'Amministrazione, tenendo conto di eventuali vincoli temporali ed architetturali di dettaglio oltre che di specifiche esigenze di customizzazione.

Per l'intero periodo di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

- Un **Project Manager Contratto di Adesione**, che coordina le attività e collabora col referente che ogni singola PA dovrà indicare e mettere a disposizione;
- Un **Technical Team Leader** che segue tutte le fasi più strettamente legate agli aspetti operativi.

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

Saranno inoltre condivisi:

- la lista dei deliverables di Progetto;
- la Matrice di Responsabilità;
- gli exit criteria di ogni fase di Progetto;
- il Modello di comunicazione tra PSN e PA.

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

- **Explore**, che include le fasi relative all'analisi e alla valutazione dell'ambiente, per aiutare la PA a definire il proprio percorso di migrazione verso il cloud.
- **Make**, che comprende tutte le attività di design e di predisposizione dell'ambiente per permettere la migrazione in condizioni di sicurezza, tra cui anche i test necessari a validare il disegno di Progetto.
- **Go**, che prevede il collaudo, l'attivazione dei servizi sulla nuova infrastruttura ed anche le attività di post go live necessarie al supporto e all'ottimizzazione dei servizi nel nuovo ambiente.

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

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

Di seguito, sono descritte le quattro fasi:

Figura 6: Servizio di Migrazione - Metodologia EMG2C

Prima di descrivere la migrazione generale dei Servizi attinenti al mondo delle prestazioni di specialistica e delle prenotazioni sanitarie, è importante evidenziare che le attuali infrastrutture disponibili, rispettivamente, su *On Premise Non Adeguato* e *IaaS Non Qualificato* presentano un insieme di vincoli architetturali conseguenti all'evoluzione negli ultimi anni e, in parte, relativi anche ad incompatibilità di alcune Applicazioni con lo stack OS Middleware. Non è stato possibile ad oggi procedere agli aggiornamenti allo stato dell'arte a causa della indisponibilità di risorse computazionali su tali infrastrutture.

In considerazione di quanto suddetto, la migrazione sul Cloud PSN prevederà una fase in modalità Re Host, idonea a preservare comunque l'operatività dei Servizi e concomitante con la seconda fase, compiuta contestualmente e progressivamente con il Re Architect che si stima di concludere al *diciottesimo Mese*, che ha l'obiettivo di adattare e ridisegnare le architetture dei Servizi attraverso un processo iterativo ed incrementale che recepisca i servizi cloud-native offerti dal Cloud del PSN per privilegiare i benefici che ne derivano.

NB. I workload di interesse saranno ospitati su infrastruttura ESAPA ovvero sul Data Center Regionale fino alla data di effettiva messa in esercizio e Go Live su PSN.

Nel seguito si descrivono le principali attività delle Fasi costituenti la Migrazione.

1. **Analisi** e **Discovery**

Il primo step consiste nell'assessment finalizzato alla raccolta delle informazioni necessarie e utili alla corretta esecuzione della migrazione, quali:

- architettura dei Servizi comprese applicazioni e dati
- finestre utili per la migrazione
- di eventuali periodi di indisponibilità dei Servizi
- analisi della sicurezza dei Servizi e delle architetture

Si utilizzerà una metodologia funzionale a identificare benefici tangibili derivanti dall'adozione del Cloud. In tale fase sarà avviata una valutazione delle architetture in esercizio per individuare e definire le correzioni funzionali a un miglioramento prestazionale.

La Discovery ha l'obiettivo di raccogliere le informazioni relative ai distinti Servizi (e alle Applicazioni da migrare) e consentirà di comporre un inventory e check list che supporteranno le successive attività e

permetteranno, in fase di collaudo, la verifica delle componenti migrate.

L'analisi permetterà anche di consolidare le infrastrutture target, eventuali vincoli, le interdipendenze da attenzionare, determinare l'allineamento agli standard tecnologici, individuare i fattori di rischio. In funzione dei risultati dell'assessment, si valuterà la migliore strategia di migrazione verso l'ambiente target con l'obiettivo di ottimizzare, laddove possibile, i tempi di migrazione e minimizzare i rischi.

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

2. **Set-up**

Rappresenta la fase propedeutica alla concreta esecuzione della migrazione, finalizzata a garantire una idonea predisposizione dell'ambiente target su cui dovranno essere migrati i Servizi dell'Amministrazione e si articola nelle seguenti fasi:

- predisposizione delle infrastrutture nel Data Center del PSN
- assegnazione delle risorse dei Servizi di cui al Par. 5.2.2
- configurazione e tuning inclusivi gli ambiti Storage, Networking e Security

Il completamento della fase di Set-up coincide con l'avvio della gestione dei Servizi.

3. **Migrazione**

Tale fase si articola nei seguenti step:

- configurazione delle risorse dimensionate in base a quanto indicato in precedenza, inclusiva dell'installazione dei Sistemi Operativi e dei software d'ambiente. La migrazione dei Servizi sarà gestita con nuove installazioni;
- tuning delle VM definito in base alle evidenze della fase di Analisi e Discovery;
- trasferimento dei workload;
- trasferimento dei dati ovvero sulle infrastrutture del PSN;
- predisposizione del Backup e definizione delle policy concordate con l'Amministrazione, schedulazione, esecuzione di test di funzionamento;
- impostazione del monitoraggio, configurazione delle utility previste per il monitoraggio delle infrastrutture/Servizi dell'Amministrazione ospitati nel Data Center del PSN.

L'on boarding dei Servizi prevede l'adozione di soluzioni tecnologiche al fine di favorire un controllo ed una razionalizzazione degli interventi.

4. Collaudo

Tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo del Servizio migrato sul Cloud del PSN. È previsto il coinvolgimento di opportuni stakeholder dell'Amministrazione

L'esecuzione del Collaudo consiste nella progettazione, pianificazione ed esecuzione dei test definiti e concordati con l'Amministrazione per certificare il Go Live della Servizi sul Cloud de PSN. In linea generale: progettazione test list (test di disponibilità, test di Integrità, test di funzionalità), esecuzione test di Collaudo che nel caso di Valida si presenteranno reiterati e ricorsivi e diretta espressione dei rilasci previsti del CUP unico nei confronti di ogni singolo soggetto erogatore.

Dopo il Collaudo sarà previsto un *grace period* temporaneo, da concordare con l'Amministrazione, durante il quale sarà fornito un supporto alle operation della Medesima per il fine tuning dei Servizi migrati in termini di prestazioni.

Il successo del Piano di Migrazione dipende dalla condivisione con l'Amministrazione dei seguenti vincoli:

- fermo applicativo: laddove la modalità di migrazione dovesse introdurre fermo applicativo, l'Amministrazione deve evidenziare la suddetta necessità e indicare finestre di intervento utili all'esecuzione della migrazione;
- config-freeze: sarà cura dell'Amministrazione comunicare una finestra temporale durante la quale non saranno eseguiti interventi di modifica delle configurazioni applicative di qualsivoglia natura (es: integrazioni, personalizzazioni, request for change) e interagire a sua cura con i Fornitori applicativi interessati per allineare la base dati allo stato dell'arte
- coinvolgimento di Attori terzi: sarà cura e responsabilità dell'Amministrazione interagire con gli eventuali Fornitori terzi per le componenti applicative al di fuori del perimetro definito nel presente Progetto ed eventualmente interconnesse con quelle oggetto di migrazione al fine di gestire le interdipendenze

NB. Si precisa ed evidenza che non è responsabilità del PSN il collaudo funzionale dei Servizi.

Nelle due seguenti tabelle sono indicate la modalità di migrazione individuate, la previsione e il dettaglio dei tempi di migrazione:

Servizio	Classificazione	Tipo di Migrazione	Previsione Tempi di Migrazione
Sistema CUP e di Gestione Analitico Sovracup	Critico	Modalità B (Re Architect)	18 Mesi
Population Health Management + Percorsi di cura Analytic Dashboard	Critico	Modalità B (Re Architect	18 Mesi
Portale Regionale Liste di Attesa	Critico	Modalità B (Re Architect	18 Mesi
SC-IAM Sanità Calabria – Identity Access Management	Critico	Modalità B (Re Architect	18 Mesi
Portale Sovracup	Critico	Modalità B (Re Architect	18 Mesi
App Mobile Sovracup	Critico	Modalità B (Re Architect	18 Mesi
Ecosistema Calabria Sanità	Critico	Modalità B (Re Architect	18 Mesi

Tabella 17: Servizi, Classificazione, Migrazione, Tempistiche

Servizio	Classificazione	T1 Analisi & Discovery	T2 Set Up	T3 Migrazione	T4 Collaudo
Sistema CUP e di Gestione Analitico Sovracup	Critico	T0 + 5 M	T1 + 3 M	T2 + (2 M) + 6 M	T3 + (4 M) + 4 M
Population Health Management + Percorsi di cura Analytic Dashboard	Critico	T0 + 5 M	T1 + 3 M	T2 + (2 M) + 6 M	T3 + (4 M) + 4 M
SC-IAM Sanità Calabria – Identity Access Management	Critico	T0 + 5 M	T1 + (1 M) + 1 M	T2 + 8 M	T3 + (4 M) + 4 M
Portale Regionale Liste di Attesa	Critico	T0 + 5 M	T1 + 3 M	T2 + (2 M) + 6 M	T3 + (4 M) + 4 M
Portale Sovracup	Critico	T0 + 4 M	T1 + 2 M	T2 + (1) + 2 M	T3 + (1) + 4 M
App Mobile Sovracup	Critico	T0 + 4 M	T1 + 2 M	T2 + (1) + 2 M	T3 + (1) + 4 M
Ecosistema Calabria Sanità	Critico	T0 + 4 M	T1 + 2 M	T2 + (1) + 2 M	T3 + (1) + 4 M

Tabella 18: Servizi e tempistica Fasi di Migrazione

Di seguito, una descrizione sintetica del Piano di Migrazione di massima definito per i Servizi indicati nelle precedenti due tabelle per la quale sarà definita la strategia di migrazione B.

Analisi e Discovery

- Analisi di dettaglio riferita all'AS IS dello stato architetturale in termini di componenti, interazioni e vincoli tecnologici;
- decomposizione delle Applicazioni tramite la suddivisione in componenti all'identificazione dei singoli moduli o servizi che costituiscono le stesse;
- definizione delle dipendenze relative alle interazioni tra i diversi componenti e alle dipendenze funzionali e dei dati;
- progettazione dell'architettura cloud basata su microservizi tramite la suddivisione dell'applicazione in servizi autonomi e scalabili;

- ridisegno dei componenti con l'adattamento degli stessi all'architettura cloud e all'ambiente cloud definiti nel corso della progettualità.

Set-up

- Gestione dello stato e del dato tramite l'adattamento dei dati finalizzati a sfruttare i servizi di archiviazione cloud;
- aggiornamento del codice per consentire la corretta integrazione delle risorse di archiviazione cloud nei componenti. In queste attività potrebbe essere inclusa la riorganizzazione delle directory, l'aggiornamento delle librerie e la gestione delle relative dipendenze;
- riadattamento delle porzioni di codice incompatibili con l'ambiente cloud o che potrebbero richiedere la riscrittura per sfruttare al meglio le risorse cloud;
- *auto scaling* per mezzo della configurazione dell'ambiente cloud alfine di aumentare o ridurre automaticamente le risorse in base al carico dell'applicazione;
- adozione di lambda-function funzionali alla scomposizione della piattaforma AS IS in modalità service-oriented per sfruttare la capacità di autoscaling e di orchestrazione delle risorse PSN
- utilizzo di API gateway per favorire l'interoperabilità con sistemi esterni e altre tecnologie
- trasformazione dell'applicativo AS IS in componenti stateful e stateless
- creazione di un layer di integrazione per rispettare il principio di Once Only ed evitare la duplicazione dei dati funzionali al runtime della e terze piattaforme nazionali, consentendone il recupero direttamente dalle sorgenti primarie.
- bilanciamento del carico con la ridistribuzione del traffico tra istanze multiple al fine di evitare sovraccarichi e garantirne la disponibilità;
- configurazione di strumenti e framework per lo sviluppo, con relativo *versioning* del codice e la gestione dei rilasci;
- creazione di ambienti di test per valutare gli interventi senza influire sulla produzione del nuovo *versioning* dei sistemi.

Migrazione (Esecuzione)

Rappresenta la fase centrale del processo in cui saranno apportate modifiche e miglioramenti all'architettura esistente. Nello specifico,

- sviluppo delle componenti architetturali, funzionali e di sistema finalizzate ad incrementare le funzionalità e ottimizzare il sistema, parallelamente alla predisposizione in ottica del servizio in modalità cloud;
- esecuzione di test approfonditi finalizzati a verificare che i componenti adattati funzionino correttamente nell'ambiente cloud;
- esecuzione dei test di integrazione e dei test funzionali finalizzati a garantire che i componenti interagiscano correttamente tra loro e con i servizi cloud;
- esecuzione di test approfonditi, compresi test di carico, prestazioni e tolleranza ai guasti.
- pianificazione ed esecuzione della migrazione per lo spostamento dei dati esistenti e la configurazione delle risorse cloud necessarie alla messa in atto del sistema;
- deployment della nuova architettura nell'ambiente di produzione;
- rilascio graduale per minimizzare l'impatto sugli utenti.

Collaudo

Nel corso della fase di Collaudo saranno monitorati i parametri e gli out come di processo a seguito del rilascio dei servizi a seguito del Re-Architect e saranno eseguite attività di:

- implementazione di piani e strumenti di monitoraggio finalizzati a raccogliere dati sulle prestazioni e identificare eventuali problemi;
- ottimizzazione dell'uso delle risorse cloud per garantire efficienza;
- supporto

5.4.1 Piano di attivazione e Gantt

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

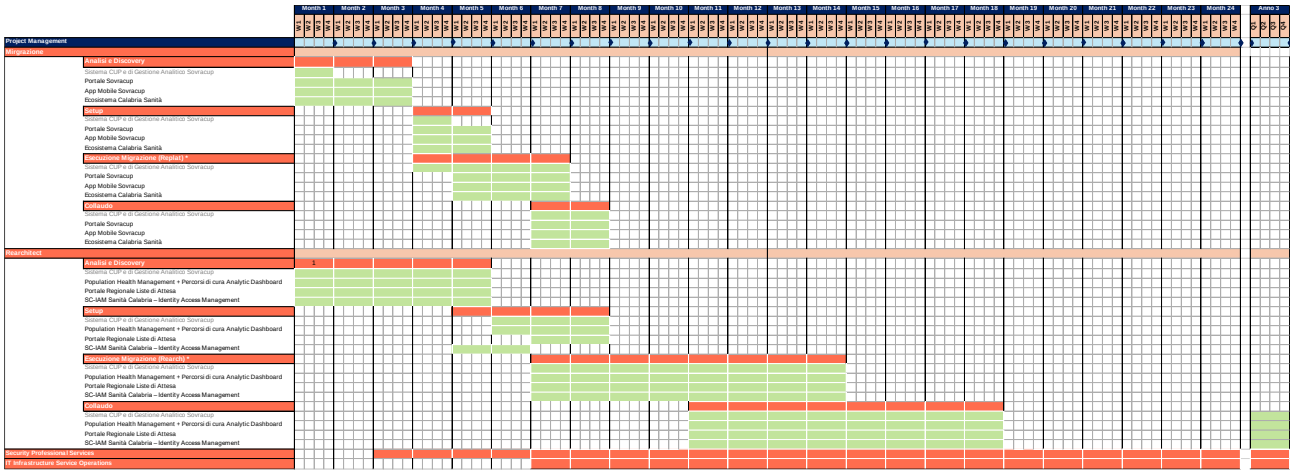

Figura 7 Piano di Attivazione e Gantt

Come indicato in precedenza, il completamento della fase di Set-up coincide con l'avvio della fase di gestione dei Servizi.

Per i sette Servizi descritti in precedenza,

- Servizi Sistema CUP e di Gestione Analitico Sovracup,
- Population Health Management + Percorsi di cura Analytic Dashboard,
- SC-IAM Sanità Calabria – Identity Access Management,
- Portale Sovracup,
- App Mobile Sovracup,
- Portale Regionale Liste di Attesa

si procederà prima ad una fase di Migrazione sul Cloud del PSN stimata in circa otto Mesi e, contestualmente, inizierà la seconda di gestione ed esecuzione delle attività d Re Achitect stimata in circa 18 Mesi.

Si ribadisce che nel presente Progetto,

- è esclusa la fornitura di Software (intese Licenze d'Uso commerciali e/o gratuite) a completamento della configurazione dei Servizi Cloud;
- è vincolante che l'Amministrazione abbia la disponibilità delle Licenze Oracle Enterprise Edition nella versione Unlimited Socket, ultima o penultima versione dichiarata da Oracle, comprensive del RAC e degli altri prodotti software idonei e completi degli strumenti a supporto del Servizio Oracle DB
- non sono comprese
    - forniture del Servizio di Connettività e Router e dei Certificati (nominativi e di tipo wildcard) SSL/TLS per la fruizione dei Servizi, compresa la loro gestione (acquisto, rinnovo, cessazione);
    - postazioni di lavoro;
    - quanto non indicato nel Progetto.

5.5 Servizi Professionali

Sono resi disponibili all'Amministrazione servizi di evoluzione con l'obiettivo di: ✓migliorare eventuali ambienti precedentemente migrati sulla piattaforma PSN tramite Re-Host o tramite i servizi di Housing/Hosting; ✓ supportare la migrazione di applicativi on premise verso una piattaforma cloud tecnologicamente avanzata, in modo da beneficiare delle funzionalità messe a disposizione dall'infrastruttura proposta, come sicurezza, scalabilità e ottimizzazione di costi e risorse.

In particolare, i due servizi proposti sono quelli di Re-Platform e Re-Architect, in quanto queste due strategie di migrazione sono quelle che maggiormente massimizzano i benefici per l'Amministrazione di una piattaforma cloud come quella oggetto del presente Progetto.

I due servizi si differenziano principalmente per la quantità del codice applicativo che viene modificato e, di conseguenza, per le tempistiche di attuazione. Il Re-platform modifica solamente alcuni componenti senza impattare il core dell'applicativo, mentre il Re-architect permette di portare l'applicazione in Cloud attraverso interventi puntuali sulla stessa.

Tali servizi non sono necessariamente alternativi ma possono eventualmente rappresentare fasi sequenziali di un programma di modernizzazione **applicativa**.

Per questi servizi, in base alla specifica esigenza, viene proposto un **team mix** composto dai profili professionali elencati in precedenza.

5.5.1 Re Architect

In questa sezione si riporta un diagramma di Gantt di massima per le attività previste nel La strategia di Re-architect ha come obiettivo quello di adattare l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare i servizi cloud-native offerti dal PSN per massimizzare i benefici che ne derivano. L'obiettivo è garantire i benefici attesi dall'Amministrazione e il minimo impatto per gli utenti finali. Il servizio si rende necessario, ad esempio, quando il livello di sicurezza è molto distante dallo standard minimo e realizza la modifica di moduli applicativi di un'applicazione al fine di garantirne un adeguato livello di sicurezza

Il servizio sarà disegnato rispettando i principi di design cloud-native che non solo consente di favorire la flessibilità operativa dei servizi applicativi, ma consente anche:

- un maggior riuso e velocità di implementazione
- l'utilizzo di metodologie consolidate di test (quanto più automatici) sia per le verifiche funzionali, sia per quelle di qualità e sicurezza
- l'uso di best practices di sviluppo e di progettazione (definite dal PSN) che consenta la trasformazione del codice applicativo in modo controllato
- una progettazione secondo le metodologie Secure by design

Discorso analogo vale per il monitoraggio delle applicazioni a valle di un Progetto di "re-architect". L'adozione matura di metodologie cloud-native permette all'applicazione di usufruire di piattaforme comuni di monitoraggio e manutenzione proattiva.

Di seguito sono illustrati i diversi step del processo di Re-architect.

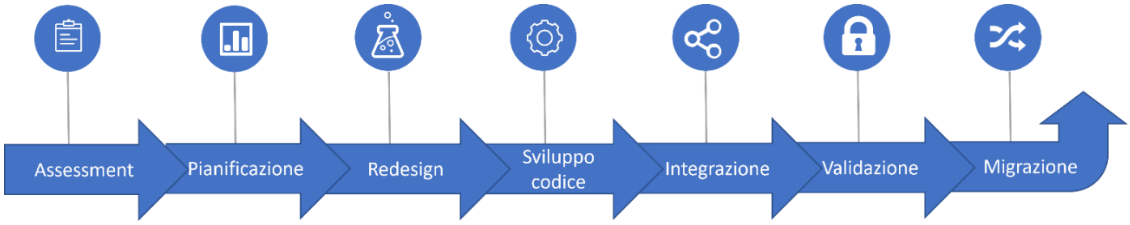

Figura 8: Flusso processo di Re-architect

Tra le attività svolte in un processo di re-architect vi è l'esecuzione dei test dei servizi PSN attivati e definiti in precedenza per certificare il Go Live delle applicazioni su ambiente target da un punto di vista infrastrutturale.

Polo Strategico Nazi

predette vulnerabilità verrà accertata e comunicata al cliente attraverso l'esecuzione di un'attività di verifica (ad es. penetration test e vulnerability assessment) eseguita prima della messa in esercizio delle componenti oggetto dei servizi di re-architect, nel rispetto delle tempistiche concordate.

5.5.2 Personalizzazione del Servizio

L'approccio individuato, basato sul principio *Low Hanging Fruit* richiede la conduzione di una puntuale analisi supportata da azioni di discovery e di prioritizzazione dei singoli componenti che costituiscono l'attuale impianto.

In particolare, alle attività di Discovery, in modesta parte condotte nelle prime fasi di progettazione, si accosta un articolato intervento caratterizzato dalla ricostruzione della conoscenza di base sugli Applicativi e sui singoli componenti prioritizzati, dall'acquisizione delle informazioni utili (sia in ambito tecnico sia di business) per supportare la strategia di migrazione di Re-Architect ritenuta indispensabile e da applicare a ciascun componente critico dei sette Servizi.

La medesima fase di analisi risulterà fondamentale per stimolare la comunicazione fra il *Personale* tecnico e non-tecnico dell'Amministrazione e delle Aziende, coinvolgendo i numerosi *Referenti* progettando i nuovi servizi con metodologie *privacy e security by design*.

Le attività di Re Architect, specificatamente per il Sistema CUP e di Gestione Analitico Sovracup, riguardano principalmente l'irrobustimento dell'infrastruttura introducendo tecnologia più recente e più efficiente in modo da supportare l'espansione sul territorio della soluzione di CUP.

Le attività sono articolate in due distinte fasi: *Centrale* e Aziende.

Nella fase *Centrale* si prevedono le attività trasversali alle Aziende Ospedaliere e Sanitarie Calabresi, tra cui la definizione di regole e specifiche comuni finalizzate all'omogeneizzazione dei processi ed alla predisposizione del sistema configurato pronto al collaudo.

Nella fase *Aziende* si prevedono le attività specifiche delle suddette Aziende, funzionali al collaudo delle integrazioni vs i sistemi Aziendali ed alla relativa messa in produzione:

1. predisposizione di un piano personalizzato per ogni Azienda, che includa i punti successivi
2. configurazione componente applicativa di base

   a. Accettazione (incluso eventuale recupero dati del solo *scheletro* agenda per le agende di accettazione, il recupero del pregresso è escluso)
   b. Cassa (incluse le regole contabili: numerazioni, causali di contabilità, conti di ricavo/credito/cassa, recupero crediti)
   c. Rendicontazione (estrattore Flusso C, LP, 730 pre-compilato, eventuale ripartizione proventi di LP, eventuale tracciato di output della ripartizione proventi)
3. predisposizione componente di integrazione
   a. integrazione vs Contabilità
   b. implementazione integrazioni verso i Dipartimentali aziendali (ove presenti, vs il Pronto Soccorso e il Laboratorio per la ricezione delle pratiche da pagare tramite il circuito MyPay, vs il RIS o le cartelle di refertazione per l'invio del prenotato/registrato e la ricezione dell'erogato)
   c. Implementazione integrazione verso MyPay/PagoPA
4. Supporto post avvio/assistenza da remoto e in presenza, in base a quanto concordato con il referente aziendale

Si precisa che:

- l'eventuale recupero dati riguarderà esclusivamente lo scheletro dell'agenda e non il pregresso degli appuntamenti, pertanto, i flussi di rendicontazione dovranno essere prodotti dal Sistema aziendale fino al mese di avvio e dal sistema regionale dallo stesso mese di avvio per la porzione di competenza;
- la gestione delle prestazioni di laboratorio è esclusa pertanto non si prevede né la possibilità d'inserimento delle pratiche né un adeguato dimensionamento infrastrutturale
- saranno implementati esclusivamente i flussi esistenti e concordati al momento dell'assessment. Eventuali nuovi flussi che l'Azienda vorrà attivare successivamente a questa fase dovranno essere oggetto di valutazione e nuova valutazione tecnica economica,

La fase *Aziende* comincia alla conclusione del collaudo previsto durante la fase *Centrale*.

Si rammenta che sono previsti cicli specifici e che ogni ciclo si presenta organico e tale da garantire l'attivazione per uno o più soggetti erogatori degli ambienti che abilitano i processi di CUP Regionale Unico.

5.5.3 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

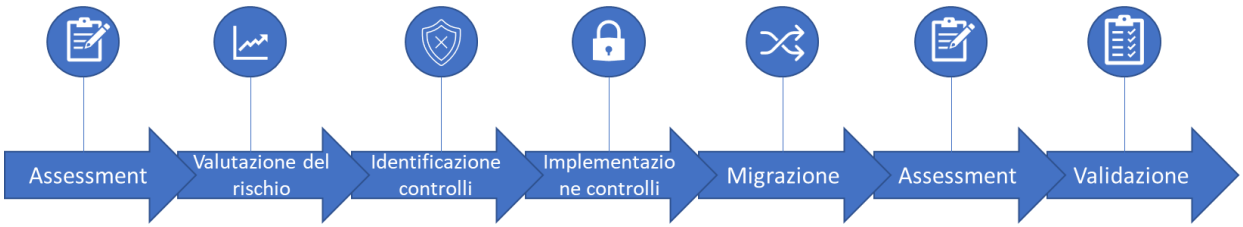

Figura 9: Flusso Security Professional Services

5.5.3.1 Personalizzazione del servizio

In linea con i principali standard normativi di riferimento nonché delle più efficaci capacità difensive attivabili nel breve/medio periodo da parte dell'Amministrazione, vengono previsti una serie di servizi orientati a migliorare la resilienza operativa, mantenere una visione in tempo reale del panorama delle minacce esistenti, predisporre reattivamente le opportune risposte a specifiche tipologie di minacce o agli incidenti di sicurezza informatica impattanti l'operatività dell'Amministrazione.

Saranno attivati i servizi professionali opportuni al fine di garantire il mantenimento dei livelli di sicurezza nel tempo, tenendo conto delle fasi del progetto di implementazione, con il servizio di **Secure Design & Activation**: un servizio di progettazione di dettaglio della definizione delle contromisure e di rilascio dei sistemi di sicurezza.

- Inoltre, saranno attivati in accordo con l'Amministrazione i seguenti servizi professionali di sicurezza:
- **Servizio di Supporto per attività di Security Device Management (Protezione Perimetrale)**: servizio orientato a supportare l'Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme di protezione perimetrale previste sulla nuova infrastruttura ICT. Il servizio è erogato "as a service" remotamente ed include la gestione degli apparati di protezione perimetrale con una finestra di servizio H8x5.
- **Servizio di supporto Device Management VCN Oracle;**
- **RTSM Security Event Monitoring, Notification & Log Management:** servizio di raccolta degli eventi di sicurezza generati dalle componenti di sicurezza allo scopo di identificare eventi potenzialmente dannosi. Valutazione prevista fino a 1500 EPS.

Inoltre, su richiesta dell'Amministrazione, potranno essere attivati i seguenti servizi erogati in modalità "a task":

- **Web Application Penetration Testing:** 1 ciclo annuo fino a 5 target (massimo 50 URL) a partire dal 2° anno;

Data la natura delle attività i servizi professionali saranno erogati secondo due principali modalità:

- Servizi "a task":
  - **Web Application Penetration Testing**.
- Servizi" Ricorrenti":
  - **Servizi di Supporto Device Management Protezione Perimetrale;**
  - **Servizio di supporto Device Management VCN Oracle;**
  - **RTSM Security Event Monitoring, Notification & Log Management.**

In particolare, per quanto riguarda i servizi a task, saranno identificate e pianificate insieme all'Amministrazione le attività di lavorazione. Per ciascun task il PSN:

- eseguirà un'analisi dei requisiti;
- definirà lo skill Mix necessario all'esecuzione;
- valuterà il dimensionamento in termini di effort per singola figura professionale ed in termini di valore economico corrispondente;
- comunicherà all'Amministrazione il risultato della propria analisi e valutazione.

Nei paragrafi seguenti vengono descritti i servizi professionali di sicurezza erogati per l'Amministrazione.

5.5.3.2 Secure Design & Activation

Il servizio consiste di un team di specialisti con le competenze e le esperienze necessarie ad effettuare l'attività di design ed implementazione delle platform Oracle FW e Oracle WAF Instance per:

- la protezione perimetrale;
- la sicurezza "by design" della nuova infrastruttura di rete;
- la raccolta e la correlazione degli eventi di sicurezza;
- l'individuazione delle vulnerabilità di sicurezza derivanti dalle debolezze architetturali;

Tale servizio viene erogato da remoto durante la fase di setup della migrazione, prevedendo un'analisi preliminare volta a comprendere le tecnologie utilizzate e le specifiche caratteristiche, al fine di poter predisporre le opportune linee guida o best practice in ambito security by design. Quest'ultime consentiranno il consolidamento dell'ipotesi di progettazione, con la successiva stesura di un piano di migrazione idoneo al contesto oggetto di studio e relativa implementazione, secondo una metodologia articolata in tre step di seguito dettagliati:

- **Step 1 – Analisi preliminare**
  In questa fase verrà eseguita un'analisi preliminare dello scenario proposto, svolgendo le seguenti attività:
  - raccolta puntuale delle informazioni sulle tecnologie attualmente utilizzate dall'Amministrazione, con i rispettivi valori di dimensionamento;
  - analisi del contesto specifico e classificazione del rischio Cyber sulla base dei livelli di criticità dei servizi a cui sono associate le specifiche tecnologie in esame;
  - analisi degli impatti di indisponibilità dei servizi, per l'individuazione delle aree problematiche e contromisure tecnologiche da adottare.
- **Step 2 – Progettazione**
  In questa fase verrà identificata l'architettura a protezione dei servizi migrati, svolgendo le seguenti attività:
  - progettazione dell'infrastruttura sulla base delle contromisure suggerite;
  - condivisione della documentazione ai referenti coinvolti.
- **Step 3 – Fase implementativa**
  In questa fase verranno condotte le attività d'implementazione delle nuove soluzioni individuate.

I deliverable prodotti consistono in attività operative corredate dalla relativa documentazione tecnica:

- Progettazione di alto livello (High Level Design) contenente tecnologie e schemi architetturali.
- Progettazione di dettaglio (Low Level Design) contenente piano di indirizzamento IP, configurazioni di dettaglio, integrazioni tra le componenti architetturali e flussi network.

Il servizio viene offerto il primo anno come supporto alla migrazione e alla riprogettazione dell'infrastruttura di rete in ottica "security by design".

5.5.3.3 Servizio di supporto per attività di Security Device Management (Protezione Perimetrale)

Il servizio professionale richiesto è orientato a supportare l'Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme di protezione perimetrale previste sulla nuova infrastruttura in perimetro PSN. Il servizio è erogato "as a service" remotamente ed include la gestione dei platform service di protezione perimetrale identificati nei servizi Oracle Network firewall e Oracle WAF Instance.

Il servizio include:

- **Presa in carico dei dispositivi:**
  - Definizione puntuale delle attività propedeutiche (accessi e utenze) ed una *timeline* di esecuzione;
  - Raggiungibilità delle platform Oracle FW e WAF e intercomunicazione con piattaforme di configuration management e log management;
  - Configurazione di utenze nominali per gli specialisti del SOC e verifica di accesso;
  - Acquisizione ed analisi di eventuali politiche generali di gestione della sicurezza perimetrale fornite dal cliente.
- **Gestione ordinaria:**
  - Esecuzione di richieste di servizio (Request Fulfillment Management) provenienti dal cliente e stakeholder di progetto, come ad esempio adeguamento e creazione politiche firewall e/o regole di esposizione/protezione servizi web; attività svolta attraverso l'elaborazione dei relativi ticket di servizio predisposti su portale TTM;
  - Verifica ed adeguamento configurazioni di logging delle platform FW e WAF in congiunzione con il servizio di Real Time Security Monitoring al fine di migliorare costantemente il livello di Detection delle minacce e delle anomalie di sicurezza;
  - Analisi e risoluzione di eventuali problematiche causate da malfunzionamenti delle platform FW e WAF e/o dalle attuali politiche di controllo del traffico di rete/applicativo.
- **Gestione straordinaria:**
  - Creazione di nuovi profili di protezione avanzata su FW e/o WAF per incremento perimetro sotto protezione.

Il servizio professionale richiesto viene erogato da remoto in una finestra temporale H8x5 gg/settimana, dal lunedì al venerdì, festivi esclusi, con annessa reperibilità degli specialisti di prodotto per interventi fuori orario necessari in caso di problematiche bloccanti. Eventuali esigenze schedulate di attività al sabato possono essere gestite all'interno del servizio di reperibilità. L'ingaggio del reperibile potrà essere fatto da altri team operativi del SOC o dal cliente tramite i canali di comunicazione che verranno concordati in fase di avvio dei servizi.

Le attività sopra indicate saranno svolte in aderenza ai seguenti processi certificati ISO20000-1:2018:

- Change Management (es. aggiornamento firmware dispositivo);
- Request Fulfillment (es. implementazione/modifica firewall policy);
- Problem Management (es. degrado delle performance di un dispositivo di sicurezza);
- Incident Management (accezione IT del temine Incident) (es. indisponibilità di un dispositivo di sicurezza).

5.5.3.4 Servizio di supporto Device Management VCN Oracle

Il servizio si articola nella gestione L3 e L4 VCN Oracle, e si declina principalmente nelle seguenti attività:

- Configurazione del logical switching secondo le necessità e le richieste del Cliente;
- Configurazione e personalizzazione delle policy FW (ACL) secondo le necessità e le richieste del Cliente;
- Gestione degli incident, attivando le procedure e gli strumenti necessari per il ripristino del servizio secondo flusso di Incident Management;
- Gestione dei problem, analizzando le anomalie, individuando e rimuovendo le cause degli stessi (problem determination);

Il servizio professionale richiesto viene erogato da remoto in una finestra temporale H8x5 gg/settimana, dal lunedì al venerdì, festivi esclusi, con annessa reperibilità degli specialisti di prodotto per interventi fuori orario necessari in caso di problematiche bloccanti. Eventuali esigenze schedulate di attività al sabato possono essere gestite all'interno del servizio di reperibilità. L'ingaggio del reperibile potrà essere fatto da altri team operativi del SOC o dal cliente tramite i canali di comunicazione che verranno concordati in fase di avvio dei servizi.

Le attività sopra indicate saranno svolte in aderenza ai seguenti processi certificati ISO20000-1:2018:

- Change Management (es. aggiornamento firmware dispositivo);
- Request Fulfillment (es. implementazione/modifica firewall policy);
- Problem Management (es. degrado delle performance di un dispositivo di sicurezza);
- Incident Management (accezione IT del temine Incident) (es. indisponibilità di un dispositivo di sicurezza).

5.5.3.5 RTSM Security Event Monitoring, Notification & Log Management

Il servizio professionale in oggetto, erogato remotamente dal Centro Servizi, garantisce in modalità continuativa (H24x365gg/anno) il monitoraggio e la gestione degli allarmi ed incidenti di sicurezza con un team di specialisti in ambito cyber (Senior Security Analyst, Security Solution Architect, Junior Security Analyst, Senior Information Security Consultant, Junior Information Security Consultant) organizzati su 2 livelli operativi (1° livello SOC e 2° livello SOC).

Il servizio utilizza una piattaforma di Security Information and Event Management (SIEM) che mette a disposizione PSN integrata con il contesto cloud di riferimento (PSN Managed – Oracle Alloy) e che, grazie a sistemi di indicizzazione e correlazione evoluti, consente il monitoraggio continuo degli eventi generati dalle componenti di sicurezza previste nel perimetro di gestione al fine di identificare rapidamente eventuali tentativi di attacco informatico o intrusioni non autorizzate.

Il servizio RTSM è dimensionato per gestire eventi e log di sicurezza raccolti dalle sorgenti indicate nella seguente tabella con un rate medio giornaliero massimo complessivo di 1.000 Eventi Per Secondo (EPS). Non è prevista la raccolta di log applicativi e l'integrazione con eventuali DB, sistemi IAM e DR presenti nel progetto.

La piattaforma SIEM sarà inoltre integrata con sorgenti di informazioni utili alla funzione di *Detection*, come ad esempio il MISP proprietario del presidio SOC.

Il servizio si articola nelle fasi di seguito descritte

- **Onboarding/Startup:** è la fase che precede l'avvio del servizio vero e proprio, e consiste nella presa in carico del perimetro del cliente attraverso le seguenti attività:
  - Revisione del perimetro di servizio (sistemi, dispositivi e appliance da monitorare o da cui acquisire log ed eventi);
  - Configurazione degli accessi remoti al perimetro oggetto di servizio;
  - Predisposizione di eventuali sonde nel perimetro oggetto di servizio deputate alla raccolta di log ed eventi della presente offerta di s.p. di sicurezza in particolare Oracle Firewall, Oracle WAF instance, EDR.
  - Definizione dei processi di comunicazione ordinaria e di escalation utilizzati nella successiva fase;
  - Redazione dei contributi di servizio utili al Service Management Plan (anche noto come Specifica di Servizio) in collaborazione con la funzione di Service Management.

  Questa fase ha una durata indicativa di 3 settimane.

- **Continous Monitoring**: è la fase continuativa del servizio ed è costituita da attività di monitoraggio degli allarmi (servizio Live/Running) e degli eventi prodotti dalle piattaforme di sicurezza dalle quali saranno estratte e analizzate le informazioni necessarie all'espletamento delle sottofasi successivamente descritte.
  - **Identification**: è la fase in cui l'analista prende in carico un allarme di sicurezza o una segnalazione e ne identifica i connotati principali al fine di procedere con la fase successiva. A titolo esemplificativo ma non esaustivo, per ogni allarme preso in gestione vengono estratti se disponibili e/o pertinenti i seguenti dati:
    - La tipologia e/o regola di correlazione ad esso associata;
    - L'indirizzo IP e/o hostname della sorgente di attacco e della vittima;
    - L'utente o gli utenti coinvolti;
    - I riferimenti temporali dell'accaduto (inizio e fine/evento in corso);
    - Lo stato del traffico e/o dell'azione (e.g. bloccato/non bloccato/non noto);
    - Breve descrizione dell'evento.

  In questa fase vengono identificati gli eventuali Falsi Positivi e vengono attivate richieste di servizio nei confronti del team operativo che amministra il SIEM al fine di migliorare la qualità della funzione di "Detection" abilitante il servizio (parte del servizio di *Continous Improvement*).

- **Classification**: è la fase in cui l'analista, dopo aver raccolto tutte le evidenze ed aver fatto una prima analisi dell'accaduto, procede con la classificazione dell'evento in termini di categoria di minaccia e di livello di gravità/pericolosità. L'assegnazione del livello di criticità ad un allarme dipende da diversi fattori, tra i quali ad esempio:
  - La tipologia di allarme/ anomalia;
  - La criticità dell'asset coinvolto, ove per asset si intende non solo un PC/Server ma anche un utente o casella di posta o dispositivo di rete;
  - Il numero di asset coinvolti.

- **Notification**: è la fase di produzione dei deliverable previsti dal primo livello di servizio ossia la fase in cui le analisi effettuate vengono tradotte in elementi di notifica (ticket IH) ed inoltrati agli interlocutori designati nei processi redatti nella fase di onboarding e costituenti il Service Management Plan.
  Il servizio di 1° livello SOC sopra descritto nelle sue fasi e sottofasi ha come obiettivo la rapida e corretta identificazione di minacce reali e la loro comunicazione agli attori interessati coerentemente con i processi di comunicazione definiti in fase di onboarding che, tra le altre cose saranno funzione degli asset coinvolti e della criticità dell'incidente rilevato.
  Di seguito, a titolo esemplificativo, viene riportato un esempio di procedura di Real Time Security Monitoring:
  - In caso di segnalazione di un evento di sicurezza dai sistemi di monitoraggio (SIEM), l'analista effettua una prima analisi sulla base delle evidenze disponibili;
  - Se l'analisi conferma che si tratta di un incidente e non di un falso positivo, viene aperto un case (ticket di Incident Handling) sul sistema di ticketing parte del servizio;
  - Il sistema di ticketing invia automaticamente la notifica ai referenti del Cliente e al presidio SOC di 2° Livello;
  - Contestualmente alla notifica vengono avviati i processi di incident handling;
  - In caso di Falso Positivo la segnalazione viene chiusa indicandone le motivazioni e viene aperta una richiesta di Tuning al gruppo di amministrazione del SIEM.

- **2° Livello SOC - Incident Handling/Response**
  Il servizio di Incident Handling/Response (presidio SOC di 2° livello), abbinato al primo livello di Real Time Security Monitoring, prevede l'esecuzione di analisi con un livello di profondità maggiore volte alla corretta identificazione della minaccia in essere e la sua estensione nel perimetro oggetto di servizio con la successiva identificazione e notifica delle attività di contenimento e risposta necessarie ai gruppi competenti (altri servizi SOC in perimetro e/o stakeholder di progetto), nonché suggerire e coordinare le azioni di eradicazione e ripristino (ove applicabili).
  Il processo di Incident Handling si chiude sul sistema di notifica messo a disposizione da PSN con il completamento del ticket IH ("Allarme reale") e contestuale apertura di eventuali service request verso altri team operativi per l'esecuzione delle azioni individuate come urgenti e necessarie (Response), con tracciamento completo delle attività e richieste sul medesimo sistema.
  Questo servizio di 2° livello SOC sarà erogato da personale con adeguata esperienza e skill nell'ambito della Incident Response (CSIRT), il quale potrà essere ingaggiato nei seguenti modi:
  - Proattivamente dal 1° livello SOC di Real Time Security Monitoring, tramite notifica di ticket (IH) di Incident Handling e contestuale chiamata telefonica in caso di priorità ALTA a seguito dell'individuazione di un fenomeno malevolo con potenziali impatti verso il cliente che necessita di analisi approfondite ed una identificazione più puntuale delle azioni di contenimento e remediation necessarie nel breve/medio/lungo periodo;
  - Reattivamente dal cliente o da uno stakeholder per segnalazione, richiesta di analisi o risposta ad un presunto incidente con impatto sui sistemi e servizi in perimetro di servizio.

- **Reporting***:* è la fase conclusiva del servizio nella quale sono fornite due tipologie di report:
  - Technical Report, ovvero una scheda incidente con tutte le indicazioni necessarie per la spiegazione dei problemi di sicurezza riscontrati e con i necessari suggerimenti relativi alle

misure più idonee da adottare per il contenimento e la risoluzione. La scheda conterrà tutte le informazioni citate nella sottofase di Identificazione ed inserite nel ticket IH sopra menzionato;

- Executive report, ovvero un rapporto periodico di sintesi elaborato congiuntamente dal Security Service Manager e destinato prevalentemente al management e al personale non tecnico che riporta una descrizione dei trend di minaccia riscontrati e gli indicatori di performance di servizio.

La tipologia e il formato del report sarà concordato in fase di delivery e messo a disposizione attraverso la piattaforma NGS su cui il presidio traccerà tutte le fasi della gestione degli incidenti.

Categorizzazione delle minacce e classificazione degli eventi

La categorizzazione delle minacce utilizzata nell'ambito del servizio in oggetto si basa sulla tassonomia ENISA; tale tassonomia è visionabile al seguente link – "*Tassonomia minaccia dell'ENISA - Data Europa EU*"[1].

All'interno di ogni segnalazione viene espressa la priorità dell'evento secondo una scala ordinale a quattro valori (Alta, Media, Bassa). Il livello di priorità è dato dal prodotto tra la criticità degli attacchi, valutata dagli analisti anche sulla base delle best practice internazionali, ed il potenziale impatto sugli Asset coinvolti e/o la criticità degli stessi definita e fornita dal cliente.

Di seguito la categorizzazione della criticità delle minacce categorizzate secondo la tassonomia ENISA attuale con relativi livelli di criticità delle medesime definiti secondo il know-how e le best practice del SOC:

5.5.3.6 Web Application Penetration Testing

Il presente paragrafo descrive il servizio professionale di Web Application Penetration Testing che sarà erogato una volta l'anno in modalità "a task" e svolto operativamente da remoto One Shot.

Le attività si compongono da un insieme di test manuali ed automatici, volti ad effettuare tentativi di intrusione sui sistemi Web in scope e delle applicazioni concordate. Su richiesta dell'Amministrazione vengono previste attività di test sfruttando eventuali vulnerabilità dei servizi in scope. Operativamente, sono previste le seguenti attività:

- tentativi d'intrusione sui sistemi WEB;
- tentativi di escalation dei privilegi, nel caso l'accesso ottenuto non fornisca privilegi amministrativi;
- in caso di penetrazione in un sistema, produzione delle relative evidenze al fine di dimostrare l'intrusione effettuata;
- descrizione dei rischi esistenti relativi alle possibilità di accesso non autorizzato ai suddetti sistemi.

Le attività sono condotte applicando metodologie globalmente riconosciute come standard de-facto per la conduzione di attività di penetration test, e in particolare le metodologie OSSTMM (Open Source Security Testing Methodology Manual) e OWASP (The Open Web Application Security Project) che definiscono le modalità per la conduzione di test completi, accurati, ripetibili e verificabili. Il test è eseguito per la ricerca di

vulnerabilità applicative ed in base alle tecnologie utilizzate dalle applicazioni, consentirà l'identificazione di tutte le categorie di vulnerabilità top 10 OWASP.

Le attività oggetto di test saranno eseguite a valle della formalizzazione dei documenti riportati sotto.

- Legal Agreement (Manleva): Un accordo stabilito tra le parti che autorizza il Security Assessment Team a svolgere le attività specifica e che lo scarica da responsabilità per eventuali danni o disservizi creati;
- Regole di Ingaggio: Documento che contiene indicazione di inizio e durata delle singole fasi, le finestre orario in cui verranno erogate le attività, l'elenco dei deliverable, l'assegnazione dei ruoli e delle responsabilità per il fornitore ed Ente e il perimetro oggetto di analisi.

Tali documenti costituiscono perimetro e modalità di esecuzione dei test e devono essere sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test.

Al termine delle attività verrà prodotto un documento denominato WAPT Results Technical Report che conterrà il report di dettaglio delle attività eseguite durante la fase di testing e le evidenze degli attacchi e delle eventuali compromissioni rilevate.

5.5.4 IT infrastructure service operations

In seguito all'avvenuta migrazione, il PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni, ovvero dell'infrastruttura VM della PA. Pertanto, l'Amministrazione potrà decidere di affidare al PSN la gestione dell'ambiente tenendo per sé solamente la componente relativa al codice applicativo. Per il corretto svolgimento delle attività verrà reso disponibile, un Service Manager; un professionista di esperienza che coordina la gestione dei servizi di gestione contrattualizzata, operando a diretto contatto con l'Amministrazione. È responsabile della qualità del servizio offerto, e costituisce un punto di riferimento diretto del cliente per analisi congiunte del servizio, escalation, chiarimenti, personalizzazioni.

Le attività che il PSN potrà prendere in carico, previa valutazione, sono:

- Monitoraggio;
- Workload management;
- Infrastructure optimization;
- Capacity management;
- Operation management;
- Compliance management;
- Vulnerability & Remediation;
- Supporto tramite la Cloud Management Platform al:
    - Provisioning, Automazione e Orchestrazione di risorse;
    - Inventory, Configuration Management.

Inoltre, potranno essere erogate attività di System Management sui sistemi operativi Microsoft e Linux e sugli ambienti middleware effettuando la gestione ordinaria e straordinaria dei Server e dei Sistemi Operativi:

- creazione/gestione delle utenze, dei privilegi e gli accessi ai sistemi;
- controllare il corretto funzionamento del Sistema Operativo, verificando i processi/servizi tramite agent di monitoring.
- gestione dei log di sistema e verifica delle eventuali irregolarità.
- gestione dei files di configurazione dei sistemi.
- problem management di 2° livello, attivando le procedure e gli strumenti necessari per l'analisi dei problemi, individuando e rimuovendo le cause degli stessi.
- effettuare il restore in caso di failure di sistema recuperando i dati di backup.
- segnalazione dell'esigenza dell'applicazione di patch/fix per il mantenimento dei sistemi agli standard di sicurezza e qualità previsti dai produttori software (segnalazione periodica o eccezionale a fronte di gravi vulnerabilità).
- applicazione delle patch/fix, sulla base di quanto concordato con il cliente o a seguito di segnalazione dagli enti deputati alla sicurezza dei sistemi e dei Data Center.

Per tali servizi verrà proposto un **team mix** composto dal mix dei profili professionali elencati in precedenza, in base all'ambiente dell'Amministrazione ed ai requisiti della stessa.

5.5.4.1 Personalizzazione del servizio

Le attività previste nel Progetto sono focalizzate unicamente sulla configurazione e gestione dell'infrastruttura abilitante i Servizi che l'Amministrazione provvederà a migrare, quali:

- eseguire attività schedulate
- assicurare il controllo sullo stato dei sistemi
- individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie
- prevenire, gestire e risolvere i problemi che comportano interruzione o degrado del servizio all'Utenza
- ottimizzare l'utilizzo delle risorse e garantire disponibilità, salvaguardia e integrità dei dati
- garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse, garantire l'adeguamento degli ambienti elaborativi a fronte di eventuali e contingenti modifiche apportate ai Servizi
- monitorare e verificare i consumi effettivi delle infrastrutture

Di seguito, le principali attività per area di intervento:

Configurazione dei Servizi Infrastrutturali

- configurazioni propedeutiche alla messa in esercizio delle VM
- installazione, configurazione e personalizzazione del Sistema Operativo in base alla necessità dell'ambiente applicativo ed alle richieste dell'Amministrazione
- configurazione ed assegnazione dello storage necessario
- configurazione ambito Network
- configurazione policy di sicurezza necessarie per la protezione dei dati
- creazione delle Utenze amministrative e non

Backup

Configurazione, attivazione, gestione e del servizio di Backup

- supporto per la definizione e configurazione delle policy di Backup
- installazione e configurazione agent
- attivazione del servizio secondo politiche concordate con l'Amministrazione
- schedulazione delle attività di Backup
- esecuzione del backup e l'eventuale funzione di Restore

System Fault & Performance Monitor

Il servizio è orientato al monitoraggio degli ambienti virtuali per garantire il corretto funzionamento delle componenti di servizio identificate a livello del sistema operativo.

Previste le seguenti attività:

- predisposizione e configurazione dei sistemi di monitoraggio management
- definizione delle specifiche di monitoraggio:
    - controllo di eventi critici, stato dei processi, performance, utilizzo delle risorse, problem determination
- azioni di ripristino e per prevenire un eventuale degrado del servizio

System Management

Comprese le seguenti attività:

- gestione ordinaria delle VM e dei sistemi operativi
- gestione dei problem, analizzando le anomalie, individuando e rimuovendo le cause degli stessi
- creazione e gestione delle Utenze, dei privilegi e degli accessi ai sistemi
- gestione dei Log di sistema
- gestione e applicazione di aggiornamenti patch/fix per il mantenimento dei sistemi agli standard di sicurezza e qualità previsti dai produttori software

Start up Middleware

Previste le seguenti attività:

- installazione, configurazione e personalizzazione del Middleware in base agli ambienti applicativi
- definizione delle specifiche di monitoraggio
- predisposizione e configurazione dei sistemi di management

Middleware Fault & Performance Monitor

Il servizio è orientato al monitoraggio del software di middleware: interviene nella sorveglianza del funzionamento delle componenti di servizio identificate a livello del software middleware.

Middleware Management

Comprese le seguenti attività

- gestione degli incident per il ripristino del servizio
- gestione ed analisi dei problem individuando e rimuovendo le cause degli stessi
- creazione e gestione delle utenze per l'accesso al middleware
- gestione dei cambiamenti da apportare all'ambiente di middleware
- gestione ed applicazione di patch/fix per il mantenimento dei sistemi agli standard di sicurezza
- tuning dei servizi applicando le eventuali configurazioni

Application Management

Il servizio implica il supporto per la gestione e la risoluzione di eventuali problemi relativi a malfunzionamenti/errori rilevati e relativi al funzionamento delle Applicazioni.

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.

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.

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.

8 CONFIGURATORE

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

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	0000002205340793
Ragione Sociale	Regione Calabria
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2024-0000002205340793-PdF-P8R1
Versione	1

VERSIONE CONFIGURATORE	5.4.2

RIEPILOGO PREZZI				
SERVIZIO	Totale UT		Totale Canone Annuale	
Industry Standard	€	-	€	597,06
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	-
Public Cloud PSN Managed			€	574.889,92
Servizi di Migrazione	€	337.587,47		
Servizi Professionali	€	7.715.782,50		
TOTALE	€	8.053.369,97	€	575.486,98

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
	MGD-GCP-001	PublicCloudPSNManaged	LicensedCloudHyperscalerTechnology	vCPUs - General Purpose N2	703			€ 83.641,5340
	MGD-GCP-011	PublicCloudPSNManaged	LicensedCloudHyperscalerTechnology	Memory - General Purpose RAM	5000			€ 64.581,0000
	MGD-GCP-020	PublicCloudPSNManaged	LicensedCloudPersistentStorageHyperscalerTechnology	Storage - Balanced PD	40000			€ 38.800,0000
	MGD-GCP-044	PublicCloudPSNManaged	LicensedCloudStorageHyperscalerTechnology	Cloud Storage - Standard Storage Regional	456700			€ 88.599,8000
	MGD-GCP-055	PublicCloudPSNManaged	Networking	Partner Interconnect Cloud Interconnect - 1Gbps VLAN attachment via Google partner	4			€ 8.448,8944
	MGD-OCP-131	PublicCloudPSNManaged	LicensedSQLeOracleHyperscalerTechnology	SQL instances - Oracle Database Cloud Service - All Editions - BYOL	174			€254.530,4712
	MGD-GCP-167	PublicCloudPSNManaged	LicensedSecurityCloudSolution	Cloud Security - Cloud Armor	6			€ 34.590,2478
	MGD-GCP-178	PublicCloudPSNManaged	LicensedSecurityCloudSolution	Cloud Operations - Logging storage (logs retained more than 30 days)	17500			€ 1.697,5000
	MGD-GCP-179	PublicCloudPSNManaged	LicensedSecurityCloudSolution	Cloud Operations - Cloud Monitoring (5K metric size, 60 metric x hours)	1			€ 0,4718
VDC_a	HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	2			€ 130,9000
VDC_a	SO01	IndustrySt andard	SistemiOperativi	Windows Server STD CORE (2 core)	4			€ 466,1600

	SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	153		€ 59.264,5500	
	SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	243		€ 76.630,0500	
	SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	213		€ 79.193,4000	
	SP-21	ServiziProfessionali	SecurityProfessionalServices	Forensic Expert	122		€ 45.359,6000	
	SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	243		€ 72.277,9200	
	SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	186		€ 48.482,7600	
	SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	302		€ 85.239,5000	
	SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	183		€ 68.039,4000	
	SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	152		€ 79.119,0400	
	SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	302		€ 127.978,5400	
	SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	153		€ 64.836,8100	
	SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	122		€ 45.359,6000	
	SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	668		€ 298.034,8800	
	SP-05	ServiziProfessionali	SecurityProfessionalServices	Cloud Security Specialist			€ -	
	SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	171		€ 66.236,8500	
	SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	188		€ 46.870,2800	
	SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	402		€ 84.436,0800	
	SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	188		€ 59.285,8000	
	SP-05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	179		€ 44.626,4900	

	SP-07	ServiziProfessionali	Rearchitect	Project Manager	632		€ 234.977,6000	
	SP-10	ServiziProfessionali	Rearchitect	DevOps Expert	1345		€ 420.487,3500	
	SP-09	ServiziProfessionali	Rearchitect	Business Analyst	608		€ 180.843,5200	
	SP-06	ServiziProfessionali	Rearchitect	Enterprise Architect	551		€ 228.835,8100	
	SP-01	ServiziProfessionali	Rearchitect	Cloud Application Architect	561		€ 217.303,3500	
	SP-04	ServiziProfessionali	Rearchitect	Cloud Application Specialist	832		€ 262.371,2000	
	SP-05	ServiziProfessionali	Rearchitect	Cloud Security Specialist	749		€ 186.733,1900	
	SP-11	ServiziProfessionali	Rearchitect	Developer (Cloud/Mobile/Front-End Developerl	2258		€ 420.665,4000	
	SP-02	ServiziProfessionali	Rearchitect	Database Specialist and Administrator	949		€ 236.595,1900	
	SP-12	ServiziProfessionali	Rearchitect	System and Network Administrator	935		€ 278.106,4000	
	SP-08	ServiziProfessionali	Rearchitect	UX Designer	591		€ 175.787,0400	
	SP-23	ServiziProfessionali	ITInfrastructureServiceOperation	Systems Architect	1259		€ 609.028,6600	
	SP-24	ServiziProfessionali	ITInfrastructureServiceOperation	Product/Network/Technical Specialist	4630		€1.551.142,6000	
	SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	1329		€ 331.332,9900	
	SP-05	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Security Specialist	1173		€ 292.440,6300	
	SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	3158		€ 939.315,5200	

9 Rendicontazione

Di seguito, è 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 fatturazione dei servizi di seguito indicati avverrà in base alle modalità canoniche del Contratto di Utenza del PSN.

Nella seguente tabella è indicato il riepilogo, la quantità e l'importo economico delle Figure Professionali suddivise per tipologia di Servizio:

Servizio Professionale	Quantità	Una Tantum
Migrazione	1.215	€ 337.587,47
Re Architect	10.011	€ 2.842.706,05
Security Professional Services	3.042	€ 1.149.816,05
IT Infrastructure-Service Operations	11.549	€ 3.723.260,40
	Totale (IVA Esclusa)	**€ 8.053.369,97**

Tabella 19: Riepilogo Servizi Professionali

Di seguito, l'ipotesi di Rendicontazione dei Servizi Professionali distribuita nei mesi definita per la vigenza contrattuale proposta all'Amministrazione:

Servizi di Migrazione (Milestone Based)	Peso	Importo	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12	Month 13	Month 14	Month 15	Month 16	Month 17	Month 18	Month 19	Month 20	Month 21	Month 22	Month 23	Month 24	Month 36
		337.587,47 €																									
- Analisi & Discovery	18%	€ 61.379,54		€ 15.344,89		€ 15.344,89		€ 15.344,89		€ 15.344,89																	
- Setup	27%	€ 92.069,31		€ 23.017,33		€ 23.017,33		€ 23.017,33		€ 23.017,33																	
- Migrazione(*)	36%	€ 122.759,08		€ 30.689,77		€ 30.689,77		€ 30.689,77		€ 30.689,77																	
- Collaudo(*)	18%	€ 61.379,54		€ 15.344,89		€ 15.344,89		€ 15.344,89		€ 15.344,89																	
Servizi di Rearchitect (Milestone Based)		2.842.706,05 €																									
- Analisi & Discovery	20%	€ 568.541,21		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25		€ 63.171,25							
- Setup	16%	€ 454.832,97		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00		€ 50.537,00							
- Migrazione(*)	32%	€ 909.665,94		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99							
- Collaudo(*)	32%	€ 909.665,94		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99		€ 101.073,99							
Servizi professionali (canone mensile avanzamento/task)		4.873.076,45 €																									
- Security Professional Services (**)	100%	€ 1.149.816,05				€ 229.963,21		€ 229.963,21		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64		€ 45.992,64	€ 275.955,85
- IT Service Operation(**)	100%	€ 3.723.260,40				€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32		€ 219.015,32	€ 1.314.091,91
Totale		8.053.369,97 €																									

Tabella 20: Rendicontazione - Ipotesi

In riferimento all'ipotesi di Rendicontazione prevista per i Servizi Professionali saranno previsti Stati di Avanzamento Lavoro (SAL) mensili o bimestrali, da definire con l'Amministrazione, in linea con l'effettivo impegno erogato in termini di giorni uomo delle relative Figure Professionali.

La Migrazione dei Servizi sarà compiuta in un periodo complessivo approssimativamente stimato di diciotto Mesi con la pianificazione di massima indicata nel Gantt al Paragrafo 5.4.1 Ciascuna delle fasi sarà rendicontata a seguito del completamento della relativa milestone indicata nella suddetta tabella,

Nella tabella sottostante sono indicati gli Importi Economici (IVA esclusa) relativi ai Servizi Cloud Industry Standard e Professionali distribuiti nei 10 Anni:

Anno	Public Cloud PSN Managed	Servizi Professionali
1	**€ 431.615,24** *	**€ 3.925.705,77**
2	**€ 575.486,98**	**€ 2.537.616,44**
3	**€ 575.486,98**	**€ 1.590.047,76**
4	€ 575.486,98	€ -
5	€ 575.486,98	€ -
6	€ 575.486,98	€ -
7	€ 575.486,98	€ -
8	€ 575.486,98	€ -
9	€ 575.486,98	€ -
10	€ 575.486,98	€ -

Tabella 21: Rendicontazione Annuale

* I Canoni del Servizio Public Cloud PSN Managed Oracle Cloud, nel primo anno, decorreranno dalla data di attivazione che si presume dal quarto Mese dall'avvio delle attività.

I Servizi Professionali sono stati valutati per i primi tre anni: i successivi saranno definiti con una *valutazione tecnica economica personalizzata* in base alle future e specifiche esigenze dell'Amministrazione.

I Security Professional Services saranno consuntivati con SAL mensili o bimestrali e rendicontati dal *quarto Mese* fino al *trentaseiesimo Mese*

I Servizi Professionali IT Infrastructure Service Operation per il supporto alla gestione dei Servizi Cloud saranno consuntivati con SAL mensili o bimestrali e rendicontati dal *quarto Mese* fino al *trentaseiesimo Mese*.

CONCESSIONE

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

CONTRATTO DI UTENZA

SOMMARIO

CONTRATTO DI UTENZA

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

TRA

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

E

La Società **Polo Strategico Nazionale S.p.A** ("**PSN S.p.A**.") con sede legale in Roma, via G. Puccini 6, numero di iscrizione nel Registro delle Imprese di Roma 1678264, Codice Fiscale e Partita IVA 16825251008 in persona del dott. 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 **<** [•][•][•] ***da compilare a cura dell'Amministrazione>***, l'Amministrazione Utente presentava al Concessionario il proprio Piano dei Fabbisogni, così come definito all'art. 2, lett. zz. della Convenzione, contenente, per ciascuna categoria di Servizi, indicazioni di tipo quantitativo con riferimento a ciascun servizio che la stessa intende acquistare in cambio del pagamento di un prezzo.

11. Il giorno **<** [•][•][•] ***da compilare a cura dell'Amministrazione>***, il Concessionario ha presentato all'Amministrazione Utente il Progetto del Piano dei Fabbisogni, così come definito all'art. 2, lett. eee. della Convenzione, nel quale sono raccolte e dettagliate le richieste dell'Amministrazione Utente, contenute nel Piano dei Fabbisogni, e la relativa proposta tecnico/economica secondo le modalità tecniche ed i listini previsti rispettivamente nel Capitolato Servizi e nel Catalogo Servizi.

12. Il giorno **<** [•][•][•] ***da compilare a cura dell'Amministrazione>*** , il Concessionario ha presentato all'Amministrazione Utente il Piano di Migrazione di Massima, così come definito all'art. 2, lett. aaa. della Convenzione, contenente l'ipotesi di migrazione del Data Center dell'Amministrazione Utente nel Polo Strategico Nazionale.

13. In applicazione di quanto stabilito all'art. 5 della Convenzione, l'Amministrazione Utente intende aderire alla Migrazione, come definita all'art. 2, lett. qq. della Convenzione stessa, per la realizzazione del Piano dei Fabbisogni presentato al Concessionario, attraverso la stipula di apposito Contratto, come definito alla lett. q. del medesimo articolo.

14. L'Amministrazione Utente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto ivi inclusa la comunicazione trasmessa al Concessionario, riguardante la richiesta di rilascio della garanzia definitiva, prevista all'art.26 della Convenzione, secondo lo schema standard messo a disposizione da parte del Concessionario ***[Nota: L'Amministrazione Utente per permettere al PSN di rilasciare la garanzia definitiva, preventivamente alla stipula, dovrà comunicare formalmente a PSN la richiesta di procedere con l'emissione della stessa, indicando l'importo da garantire e la durata. Per tale comunicazione PSN ha predisposto un testo standard di comunicazione che sarà trasmesso all'Amministrazione unitamente al Progetto del Piano dei fabbisogni. A seguito del rilascio della garanzia, PSN ne darà comunicazione all'Amministrazione tramite PEC].***

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

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

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

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

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

SEZIONE I - DISPOSIZIONI GENERALI

Articolo 1
PREMESSE E DOCUMENTI CONTRATTUALI

1. Le premesse e gli allegati, ancorché non materialmente allegati al Contratto, ne costituiscono parte integrante e sostanziale.

2. Costituiscono, altresì, parte integrante e sostanziale del Contratto:

   a) la Convenzione e i relativi allegati;

   b) il Progetto del Piano dei Fabbisogni, redatto dal Concessionario e accettato dall'Amministrazione Utente ai sensi dei successivi artt. 6 e 7.

3. Per tutto quanto non espressamente regolato dal Contratto, trovano applicazione la Convenzione, inclusi i relativi allegati, oltre alle norme generali di riferimento di cui al successivo art. 29.

Articolo 2
DEFINIZIONI

1. I termini contenuti nel Contratto, declinati sia al singolare, sia al plurale, hanno il significato specificato nella Convenzione e nei relativi allegati.

Articolo 3
OGGETTO DEL CONTRATTO

1. Il Contratto regola le specifiche condizioni di fornitura all'Amministrazione Utente dei Servizi indicati dal Progetto del Piano dei Fabbisogni, redatto dal Concessionario e accettato dall'Amministrazione Utente ai sensi dei successivi artt. 6 e 7.

Articolo 4
DURATA DEL CONTRATTO

1. Il Contratto ha la durata complessiva di anni 10 (dieci), a decorrere dalla data di avvio della gestione del Servizio, come individuata dal successivo art. 8.

2. Le Parti espressamente concordano che, in caso di proroga della Convenzione, il Contratto si intenderà prorogato di diritto per una durata corrispondente a quella della proroga della Convenzione.

3. Resta inteso che, in nessun caso, la durata del Contratto potrà eccedere la durata della Convenzione.

SEZIONE II – ATTIVITÁ PRODROMICHE ALL'AVVIO DELLA GESTIONE DEL SERVIZIO

Articolo 5
NOMINA DEI REFERENTI DELLE PARTI

1. Entro 10 (dieci) giorni dalla stipula del Contratto:

   a) il Concessionario si impegna a nominare un Direttore del Servizio e un Referente del Servizio, così come definiti all'art. 2, lett. x. e kkk. della Convenzione;

   b) l'Amministrazione Utente si impegna a nominare un Direttore dell'Esecuzione ("**DEC**"), così come definito all'art. 2, lett. w. della Convenzione.

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

3. Entro 30 (trenta) giorni, le Parti istituiranno il Comitato di Contratto di Adesione ("Comitato"), presieduto dal Direttore del Servizio, a cui partecipano il RUP e il DEC dell'Amministrazione Utente, con il coinvolgimento dei referenti tecnici e delle figure di riferimento delle Parti. Tale Comitato viene riunito, periodicamente o a fronte di particolari esigenze, per condividere lo stato della fornitura con tutti gli attori coinvolti nel governo dei servizi, per monitorare i livelli di servizio contrattuali al fine di individuare eventuali misure correttive/migliorative nell'ottica del Continuous Service Improvement.

Articolo 6
PREDISPOSIZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO

1. Entro 60 (sessanta) giorni dalla stipula del Contratto, il Concessionario dovrà trasmettere all'Amministrazione Utente il Piano di Migrazione di Dettaglio, come definito all'art. 2, lett. bbb. della Convenzione, redatto sulla base del Progetto del Piano dei Fabbisogni e del Piano di Migrazione di Massima presentato all'Amministrazione Utente e contenente le attività e il piano temporale di dettaglio relativi alla migrazione del Data Center dell'Amministrazione Utente nel PSN.

2. Resta inteso che l'Amministrazione Utente si impegna, per quanto di propria competenza, a collaborare con il Concessionario alla redazione del progetto di dettaglio di cui al comma precedente, nonché degli eventuali allegati, e a fornire tempestivamente il supporto che si rendesse necessario, nell'ottica di garantire in buona fede il tempestivo avvio della gestione del Servizio.

Articolo 7
ACCETTAZIONE DEL PIANO DI MIGRAZIONE DI DETTAGLIO

1. L'Amministrazione Utente è tenuta a comunicare al Concessionario l'accettazione del Piano di Migrazione di Dettaglio, entro 10 (dieci) giorni dalla presentazione dello stesso.

2. È fatta salva la possibilità per l'Amministrazione Utente di presentare osservazioni al Piano di Migrazione di Dettaglio, nel termine di 10 (dieci) giorni dalla ricezione, con solo riferimento alle modalità di esecuzione delle attività di Migrazione e alla relativa tempistica, dettate da specifiche oggettive esigenze dell'Amministrazione Utente stessa.

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

4. Tenuto conto delle risultanze del dialogo di cui al comma 3 del presente articolo, il Concessionario provvederà alle conseguenti modifiche al Piano di Migrazione di Dettaglio, nei 10 (dieci) giorni successivi alla ricezione delle osservazioni.

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

SEZIONE III – FASE DI GESTIONE DEL SERVIZIO

Articolo 8
AVVIO DELLA FASE DI GESTIONE DEL SERVIZIO

1. Il Concessionario è tenuto a dare avvio alla fase di gestione del Servizio nel rispetto dei termini previsti dal Piano di Migrazione di Dettaglio di cui all'art. 6, accettato dall'Amministrazione Utente ai sensi del precedente art. 7.

2. Resta inteso che l'Amministrazione Utente presterà la propria piena collaborazione per l'ottimizzazione della Migrazione, se del caso obbligandosi a far sì che tale collaborazione sia prestata in favore del Concessionario da parte di ogni altro soggetto preposto alla gestione dei centri per l'elaborazione delle informazioni (CED) e dei relativi sistemi informatici dell'Amministrazione Utente stessa, anche laddove gestiti da società *in house*.

3. Resta, altresì inteso che al Concessionario non potranno essere addebitate penali per eventuali ritardi nell'avvio della gestione, qualora tali ritardi siano imputabili all'Amministrazione Utente, anche per il caso di inadempimento a quanto previsto dal comma precedente.

Articolo 9
MODALITÁ DI PRESTAZIONE DEL SERVIZIO

1. I Servizi oggetto del Contratto, per come individuati dal progetto di dettaglio di cui all'art. 6, dovranno essere prestati nel rispetto di quanto previsto dal Contratto stesso, nonché della Convenzione e del Capitolato Servizi, al fine di garantire il rispetto dei Livelli di Servizio ("LS" o "SLA"), descritti nell'Allegato H "Indicatori di Qualità" alla Convenzione.

2. La specificazione degli inadempimenti che comportano, relativamente alle attività oggetto della Convenzione, l'applicazione delle penali, nonché l'entità delle stesse, sono disciplinati nell'Allegato H – "Indicatori di Qualità" alla Convenzione.

Articolo 10
CORRISPETTIVO PER IL SERVIZIO

1. Il Concessionario applicherà i prezzi contenuti nel Catalogo dei Servizi e le condizioni di cui al Capitolato Servizi per ciascuno dei Servizi oggetto del presente Contratto, la cui somma complessiva, prevista nel Progetto del Piano dei Fabbisogni, costituisce il Corrispettivo massimo del Servizio, fatte salve le variazioni che derivino dalle modifiche di cui al successivo art. 13 e quanto previsto all'art. 5 comma 4 lettera ii, all'art. 5 comma 6 e all'art. 11 della Convenzione

2. Si chiarisce che ogni corrispettivo o importo definito nel presente Contratto o nei suoi allegati deve intendersi oltre IVA, se dovuta.

Articolo 11
PERIODICITÀ DEI PAGAMENTI E FATTURAZIONE

1. Fermo restando quanto previsto dall'art. 24 della Convenzione, il Corrispettivo del Servizio, determinato ai sensi del precedente art. 10, è versato dall'Amministrazione Utente al Concessionario, con cadenza bimestrale posticipata, a partire dalla data di avvio della fase di gestione, per come individuata ai sensi del precedente art. 8, e a fronte dell'effettiva fornitura del Servizio nel bimestre di riferimento, secondo quanto previsto dal presente Contratto, secondo quanto disposto dal precedente art. 9.

2. Entro 10 (dieci) giorni dal termine del bimestre di riferimento, la fattura relativa ai corrispettivi maturati viene emessa ed inviata dal Concessionario all'Amministrazione Utente, la quale procederà al relativo pagamento entro 30 (trenta) giorni dalla ricezione.

3. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti percentuali, secondo quanto previsto dall'art. 5 del d. lgs. n. 231/2002.

4. L'Amministrazione Utente potrà operare sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5% (zerovirgolacinque per cento) che verrà liquidata dalla stessa solo al termine del presente Contratto e previa acquisizione del documento unico di regolarità contributiva.

5. Fermo restando quanto previsto dall'art. 30, commi 5, 5-*bis* e 6 del d. lgs. n. 50/2016 e ss.mm.ii. (rubricato Codice dei contratti pubblici) ("**DLGS 50/2016**")e dall'art. 24 della Convenzione, in relazione al caso di inadempienze contributive o retributive, e relative trattenute, i pagamenti avvengono dietro presentazione di fattura fiscale, con modalità elettronica, nel pieno rispetto degli obblighi di tracciabilità dei flussi finanziari, di cui all'art. 3, legge 13 agosto 2010, n. 136 e successive modificazioni o integrazioni, mediante bonifico bancario sul conto n. 1000/00136942 presso Intesa San Paolo S.p.A., IBAN: IT13V0306901000100000136942 o, fermo il rispetto delle norme sulla tracciabilità dei flussi finanziari, su altro conto corrente intestato al Concessionario e previa indicazione di CIG e, qualora acquisito, di CUP nella causale di pagamento. I soggetti abilitati a operare sul conto sopra riportato per conto del Concessionario sono: l'Amministratore Delegato, dott. Emanuele Iannetti e il Chief Financial Officer, dott. Antonio Garelli.

Articolo 12
MODIFICHE IN CORSO DI ESECUZIONE

1. L'Amministrazione Utente ha la facoltà di richiedere per iscritto modifiche in corso di esecuzione per far fronte ad eventuali nuove e diverse esigenze emerse in fase di attuazione.

2. Qualora le modifiche proposte riguardino il Piano di Migrazione di Dettaglio, nel termine di 30 (trenta) giorni dalla ricezione delle richieste di modifica, il Concessionario presenterà all'Amministrazione Utente un nuovo Piano di Migrazione di Dettaglio. L'Amministrazione Utente provvederà all'accettazione secondo la procedura delineata dall'art. 7 del presente Contratto. Tali variazioni sono adottate in tempo utile per consentire al Concessionario di garantire l'erogazione dei servizi.

3. Qualora le modifiche proposte riguardino il Progetto del Piano dei Fabbisogni trovano applicazione, in quanto compatibili, gli art. 106, comma 2 e 175, comma 4 del **DLGS 50/2016**.

4. Nel caso in cui le modifiche proposte ai sensi del comma precedente non superino la soglia di cui al 10% (dieci per cento) del valore iniziale del Contratto, l'Amministrazione Utente procederà con la presentazione al Concessionario di un nuovo Piano dei Fabbisogni, sulla base del quale il Concessionario redigerà un nuovo Progetto del Piano dei Fabbisogni, che sarà poi accettato dall'Amministrazione Utente secondo la procedura delineata all'art. 18 della Convenzione. Il Progetto del Piano dei Fabbisogni accettato dall'Amministrazione Utente a norma del presente comma sostituirà il progetto originario allegato al presente Contratto. La predisposizione del Piano di Migrazione di Dettaglio conseguente segue la procedura delineata all'art. 7 del presente Contratto.

Articolo 13
VERIFICHE IN CORSO DI ESECUZIONE

1. Fermo quanto previsto dalla Convenzione, l'Amministrazione Utente avrà facoltà di eseguire verifiche relative al rispetto di quanto previsto dal Contratto stesso, della Convenzione e dei Livelli di Servizio ("LS" o "SLA"), descritti nell'Allegato H "Indicatori di Qualità" alla Convenzione.

2. Il Concessionario si impegna a collaborare, per quanto di propria competenza, con l'Amministrazione Utente, fornendo tempestivamente il supporto che si rendesse necessario, nell'ottica di garantire in buona fede l'efficiente conduzione delle attività di verifica di cui al comma precedente.

3. Le risultanze delle attività di verifica saranno comunicate al Direttore del Servizio del Concessionario perché siano eventualmente discusse in contraddittorio con il Direttore dell' Esecuzione e gli eventuali ulteriori rappresentanti dell'Amministrazione Utente, sia laddove si presentino delle criticità, perché si individuino in modo collaborativo le misure adatte al loro superamento, sia perché possano formare oggetto di conoscenza e miglioramento della *performance* laddove mettano in luce elementi positivi suscettibili di ulteriore implementazione o estensione.

Articolo 14
PROCEDURA DI CONTESTAZIONE DEI DISSERVIZI E PENALI

1. Fermo restando quanto previsto dagli artt. 21 e 23 della Convenzione, la ritardata, inadeguata o mancata prestazione dei Servizi a favore dell'Amministrazione Utente secondo quanto previsto dal presente Contratto comporta l'applicazione delle penali definite in termini oggettivi in relazione a quanto dettagliato all'Allegato H - "Indicatori di Qualità" alla Convenzione.

2. Il ritardato, inadeguato o mancato adempimento delle obbligazioni di cui al presente Contratto che siano poste a favore dell'Amministrazione Utente deve essere contestato al Direttore del Servizio.

3. La contestazione deve avvenire in forma scritta e motivata, con precisa quantificazione delle penali, nel termine di 8 (otto) giorni dal verificarsi del disservizio.

4. In caso di contestazione dell'inadempimento, il Concessionario dovrà comunicare per iscritto le proprie deduzioni, all'Amministrazione Utente entro 10 (dieci) giorni dalla ricezione della contestazione stessa. Laddove il Concessionario non contesti l'applicazione della penale a favore dell'Amministrazione Utente, il Concessionario provvederà, entro e non oltre 60 (sessanta) giorni, a corrispondere all'Amministrazione Utente la somma dovuta; decorso inutilmente il termine di cui al presente comma, l'Amministrazione Utente potrà provvedere ad incassare le garanzie nei limiti dell'entità della penale.

5. A fronte della contestazione della penale da parte del Concessionario, il Direttore 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 **DLGS 50/2016**. Lo svincolo è automatico, senza necessità di nulla osta dell'Amministrazione Utente, con la sola condizione della preventiva consegna all'istituto garante, da parte del Concessionario, degli stati di avanzamento o di analogo documento, in originale o in copia autentica, attestanti l'avvenuta esecuzione. In ogni caso, lo svincolo avverrà periodicamente con cadenza trimestrale a seguito della presentazione della necessaria documentazione all'Amministrazione Utente secondo quanto di competenza.

4. Laddove l'ammontare della garanzia prestata ai sensi del presente articolo dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Concessionario dovrà provvedere al reintegro entro il termine di 45 (quarantacinque) giorni lavorativi dal ricevimento della relativa richiesta effettuata dall'Amministrazione Utente, pena la risoluzione del Contratto.

5. La garanzia prestata ai sensi del presente articolo è reintegrata dal Concessionario a fronte dell'ampliamento del valore dei Servizi dedotti in Contratto nel corso dell'efficacia di questo, ovvero nel caso di estensione della durata della Convenzione e/o del Contratto ai sensi dell'art. 4, comma 2 del Contratto.

Articolo 16
POLIZZE ASSICURATIVE

1. Fermo restando quanto previsto dall'art. 27 della Convenzione, il Concessionario si impegna a stipulare idonee polizze assicurative, a copertura delle attività oggetto del Contratto.

2. In particolare, ferme restando le coperture assicurative previste per legge in capo agli eventuali professionisti di cui il Concessionario si può avvalere nell'ambito della Concessione, il Concessionario ha l'obbligo di stipulare una polizza assicurativa a favore dell'Amministrazione Utente, a copertura dei danni che possano derivare dalla prestazione dei Servizi, con validità ed efficacia a far data dalla sottoscrizione del Contratto, prima dell'avvio del Servizio ai sensi dell'art. 8 del Contratto, nonché, in caso di utilizzo del servizio di *housing*, una polizza a copertura dei danni

materiali direttamente causati alle cose assicurate (c.d. All Risks), per tutta la durata del Contratto, che non escluda eventi quali incendio e furto.

Articolo 17
GARANZIE DEL CONCESSIONARIO PER I FINANZIATORI

1. L'Amministrazione Utente prende atto che il Concessionario è parte, in qualità di beneficiario, di un contratto di finanziamento a medio-lungo termine sottoscritto con un pool di primari istituti finanziatori composto da Intesa Sanpaolo S.p.A., UniCredit S.p.A., Cassa depositi e prestiti S.p.A., BPER Banca S.p.A. e Banco BPM S.p.A. (i "Finanziatori") ai fini della messa a disposizione da parte di questi ultimi delle risorse finanziarie necessarie alla parziale copertura dei costi connessi alla realizzazione e gestione del Progetto, in virtù del quale il Concessionario si è impegnato, tra l'altro, a cedere in garanzia a favore dei Finanziatori tutti i crediti di qualsiasi natura, esistenti o che possano sorgere in futuro, a qualsivoglia titolo derivanti, inter alia, dal presente Contratto (la "Cessione in Garanzia").

2. L'Amministrazione Utente, in qualità di debitore ceduto, accetta pertanto sin d'ora la Cessione in Garanzia a favore dei Finanziatori dei crediti del Concessionario che verranno a maturazione in forza del presente Contratto nei confronti dell'Amministrazione Utente. In ogni caso, resta fermo che 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 in Garanzia dei crediti derivanti dal presente Contratto, l'Amministrazione Utente potrà opporre ai Finanziatori cessionari tutte le eccezioni opponibili al Concessionario in base al presente Contratto.

3. Con l'accettazione prestata dall'Amministrazione Utente ai sensi del precedente comma 2, la Cessione in Garanzia si intenderà, per l'effetto, efficace e validamente opponibile a detta Amministrazione Utente mediante la notifica dell'atto di Cessione in Garanzia, che avrà cura di effettuare il Concessionario, senza necessità di ulteriori formalità.

SEZIONE V – VICENDE DEL CONTRATTO

Articolo 18
EFFICACIA DEL CONTRATTO

1. Il Contratto assume efficacia per il Concessionario dalla data di sua sottoscrizione, per l'Amministrazione Utente dalla data della registrazione, se prevista.

Articolo 19
RISOLUZIONE PER INADEMPIMENTO DEL CONCESSIONARIO

1. Fermo restando quanto previsto dall'art. 33 della Convenzione, l'Amministrazione Utente può dar luogo alla risoluzione del Contratto, previa diffida ad adempiere, ai sensi dell'art. 1454 Cod. Civ., comunicata per iscritto al Concessionario, ai sensi dell'art. 23 del Contratto, con l'attribuzione di un termine per l'adempimento ragionevole e, comunque, non inferiore a giorni 60 (sessanta), nei seguenti casi:

   a) riscontro di gravi vizi nella gestione del Servizio;

   b) applicazione di penali, ai sensi dell'art. 15 del Contratto, per un importo che supera il 10%

(dieci per cento) del valore del Contratto;

c) mancato reintegro della garanzia ove si verifichi la fattispecie di cui all'art. 15, commi 4 e 5 del presente Contratto.

2. In caso di risoluzione per inadempimento del Concessionario, a quest'ultimo sarà dovuto il pagamento delle prestazioni regolarmente eseguite e delle spese eventualmente sostenute la predisposizione, *set-up*, messa a disposizione o ammodernamento dell'Infrastruttura, decurtato degli oneri aggiuntivi derivanti dallo scioglimento del Contratto.

Articolo 20
REVOCA E RISOLUZIONE PER INADEMPIMENTO DELL'AMMINISTRAZIONE UTENTE

1. Fermo restando quanto previsto dall'art. 35 della Convenzione, l'Amministrazione Utente può disporre la revoca dell'affidamento in concessione dei Servizi oggetto del Contratto solo per inderogabili e giustificati motivi di pubblico interesse, che debbono essere adeguatamente motivati e comprovati, con contestuale comunicazione al Concessionario, con le modalità di cui all'art. 23 del Contratto. In tal caso, l'Amministrazione Utente deve corrispondere al Concessionario le somme di cui al comma 2 del presente articolo.

2. Qualora il Contratto sia risolto per inadempimento dell'Amministrazione Utente, non imputabile al Concessionario, ovvero sia disposta la revoca di cui al comma precedente, l'Amministrazione Utente è tenuta a provvedere al pagamento, ai sensi dell'art. 176, commi 4 e 5 del **DLGS 50/2016**, in favore del Concessionario:

a) degli importi eventualmente maturati dal Concessionario ai sensi del Contratto;

b) dei costi sostenuti per lo svolgimento delle prestazioni eseguite;

c) dei costi sostenuti per la produzione di Servizi non ancora interamente prestati o non pagati;

d) dei costi e delle penali da sostenere nei confronti di terzi, in conseguenza della risoluzione;

e) dell'indennizzo a titolo di risarcimento del mancato guadagno, pari al 10% (dieci per cento), del valore dei Servizi ancora da prestare;

3. L'efficacia della risoluzione e della revoca di cui al comma 1 del presente articolo resta in ogni caso subordinata all'effettivo integrale pagamento degli importi previsti al comma 2 da parte dell'Amministrazione Utente.

4. L'efficacia della risoluzione del Contratto non si estende alle prestazioni già eseguite ai sensi dell'art. 1458 Cod. Civ., rispetto alle quali il Concedente e l'Amministrazione Utente sono tenuti al pagamento per intero dei relativi importi.

5. Al fine di quantificare gli importi di cui al comma 2 del presente articolo, l'Amministrazione Utente, in contraddittorio con il Concessionario e alla presenza del Direttore del Servizio, redige apposito verbale, entro 30 (trenta) giorni successivi alla ricezione, da parte del Concessionario, del provvedimento di revoca ovvero alla data della risoluzione. Qualora tutti i soggetti coinvolti siglino

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

6. Senza pregiudizio per il pagamento delle somme di cui al comma 2 del presente articolo, in tutti i casi di cessazione del Contratto diversi dalla risoluzione per inadempimento del Concessionario, quest'ultimo ha il diritto di proseguire nella gestione ordinaria dei Servizi, incassando il relativo corrispettivo, sino all'effettivo pagamento delle suddette somme.

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

Articolo 21
RECESSO

1. Fermo restando quanto previsto dall'art. 36 della Convenzione, in caso di sospensione del Servizio per cause di Forza Maggiore, ai sensi dell'art. 19 della Convenzione, protratta per più di 90 (novanta) giorni, ciascuna delle Parti può esercitare il diritto di recedere dal Contratto.

2. Nei casi di cui al comma precedente, l'Amministrazione Utente deve, prontamente e in ogni caso entro 30 (trenta) giorni, corrispondere al Concessionario l'importo di cui all'art. 20, comma 2 del Contratto, con l'esclusione, ai sensi di quanto previsto dall'art. 165, comma 6 del **DLGS 50/2016**, degli importi di cui alla lettera c) di cui al citato art. 20, comma 2 del Contratto.

3. Nelle more dell'individuazione di un subentrante, il Concessionario dovrà proseguire sempreché sia economicamente sostenibile, laddove richiesto dall'Amministrazione Utente, nella prestazione dei Servizi, alle medesime modalità e condizioni del Contratto, con applicazione delle previsioni di cui all'art. 5 della Convenzione in relazione ad eventuali investimenti e, comunque, a fronte dell'effettivo pagamento dell'importo di cui all'art. 20, comma 2 del Contratto.

4. Inoltre, fermo restando quanto previsto al precedente comma del presente articolo, il Concessionario può chiedere all'Amministrazione Utente di continuare a gestire il Servizio alle medesime modalità e condizioni del Contratto, fino alla data dell'effettivo pagamento delle somme di cui al comma 2 del presente articolo.

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

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

Articolo 22
SCADENZA DEL CONTRATTO

1. Alla scadenza del Contratto, il Concessionario ha l'obbligo di facilitare in buona fede la migrazione

dell'Amministrazione Utente verso il nuovo concessionario nella gestione dei Servizi o comunque verso l'eventuale diversa soluzione che sarà individuata dall'Amministrazione Utente, ferma restando la tutela dei suoi diritti e interessi legittimi.

SEZIONE VI – ULTERIORI DISPOSIZIONI

Articolo 23
COMUNICAZIONI

1. Agli effetti del Contratto, il Concessionario elegge domicilio in Roma, via G. Puccini 6, l'Amministrazione Utente elegge domicilio in **<** [•]. ***da compilare a cura dell'Amministrazione>***

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

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

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

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

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

Articolo 24
NORME ANTICORRUZIONE E ANTIMAFIA, PROTOCOLLI DI LEGALITÀ

1. Il Concessionario, con la sottoscrizione del Contratto, attesta, ai sensi e per gli effetti dell'art. 53, comma 16-ter del Codice antimafia, di non aver concluso contratti di lavoro subordinato o autonomo o, comunque, aventi ad oggetto incarichi professionali con ex dipendenti dell'Amministrazione Utente, che abbiano esercitato poteri autoritativi o negoziali per conto dell'Amministrazione Utente nei confronti del medesimo Concessionario, nel triennio successivo alla cessazione del rapporto di pubblico impiego.

2. ***<da compilare a cura dell'Amministrazione*** [**eventuale**: Il Concessionario, con riferimento alle prestazioni oggetto del Contratto, si impegna - ai sensi dell'art. [•] del Codice di comportamento/Protocollo di legalità [•] - ad osservare e a far osservare ai propri collaboratori a qualsiasi titolo, per quanto compatibili con il ruolo e l'attività svolta, gli obblighi di condotta previsti dal Codice di comportamento/Protocollo stesso.

3. A tal fine, il Concessionario dà atto che l'Amministrazione Utente ha provveduto a trasmettere, ai sensi dell'art. [•] del Codice di comportamento/Protocollo di legalità sopra richiamato, copia del Codice/Protocollo stesso per una sua più completa e piena conoscenza. Il Concessionario si impegna a trasmettere copia dello stesso ai propri collaboratori a qualsiasi titolo.]**>**

4. La violazione degli obblighi, di cui al presente articolo, costituisce causa di risoluzione del Contratto.

Articolo 25
OBBLIGHI IN TEMA DI TRACCIABILITÀ DEI FLUSSI FINANZIARI

1. Il Concessionario assume tutti gli obblighi di tracciabilità dei flussi finanziari, per sé e per i propri subcontraenti, di cui all'art. 3, legge 13 agosto 2010, n. 136 e ss.mm.ii., dandosi atto che, nel caso di inadempimento, il Contratto si risolverà di diritto, *ex* art. 1456 Cod. Civ..

Articolo 26
CONTROVERSIE E FORO COMPETENTE

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

Articolo 27
TRATTAMENTO DEI DATI PERSONALI

1. In materia di trattamento dei dati personali, si rinvia alla Normativa Privacy e al GDPR, come vigenti, e ai relativi obblighi per il Concessionario, descritti nell'Allegato E alla Convenzione "Facsimile nomina Responsabile trattamento dei dati personali" secondo lo schema standard messo a disposizione da parte del Concessionario con i relativi sub-allegati che opportunamente compilato e firmato dall'Amministrazione Utente per accettazione della nomina dal Concessionario diventa parte integrante del presente Contratto.

Articolo 28
REGISTRAZIONE

1. La stipula del Contratto è soggetta a registrazione presso l'Agenzia delle Entrate. Tutte le spese dipendenti dalla stipula del Contratto sono a carico del Concessionario.

Articolo 29
RINVIO AL CODICE CIVILE E AD ALTRE DISPOSIZIONI DI LEGGE VIGENTI

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

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

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

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

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

Polo Strategico Nazionale S.p.A.

Amministratore Delegato

(Emanuele Iannetti)