SERVIZIO SANITARIO NAZIONALE
REGIONE PIEMONTE
Azienda Sanitaria ZERO
Costituita con D.P.G.R. 18/02/2022 n. 9
Codice Fiscale / P.I. 12685160017
Sede legale: Via San Secondo, 29 bis – 10128 Torino

Deliberazione del Commissario
S.C. Sistema Informativo

OGGETTO: Adesione di Azienda Zero, per la realizzazione di uno spazio cloud per gli applicativi aziendali, alla convenzione avente ad oggetto la concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione, denominata Polo Strategico Nazionale (PSN). Importo complessivo di euro 366.267,18 IVA inclusa. Durata contrattuale di 60 mesi. CIG derivato A018A3E796.

Su proposta del Direttore f.f. S.C. Sistemi Informativi Azienda Zero ing. Salvatore Scaramuzzino, che di seguito si riporta:

- premesso che:

  - l'art. 1 della legge regionale 26 ottobre 2021, n. 26 (in seguito parzialmente modificata dall'art. 1 della L.R. n. 2 del 25 marzo 2022) ha previsto l'istituzione dell'Azienda Zero (di seguito denominata Azienda Zero, quale ente del Servizio Sanitario Regionale dotato di personalità giuridica pubblica e di autonomia amministrativa, patrimoniale, organizzativa, contabile, gestionale e tecnica;
  - con D.P.G.R. n. 9 del 18.02.2022 è stata costituita, ai sensi e per gli effetti della citata legge regionale 26 ottobre 2021, n. 26, l'Azienda Zero;
  - con D.G.R. n. 32-4847 del 31.03.2022 è stato disposto, nelle more dell'avvio delle procedure di selezione regionale e della nomina del Direttore Generale, il commissariamento dell'Azienda Zero, individuando il Commissario, in considerazione dell'esperienza maturata, nella persona del dott. Carlo Picco, con decorrenza dal 01.04.2022 e per il tempo strettamente necessario alla nomina del Direttore Generale, prorogato al 31.12.2023 con D.G.R. n. 17-6131 del 02.12.2022;

- dato atto che il Commissario, con deliberazione n. 2/01.00/2022 del 13.06.2022 ha approvato l'Atto Aziendale dell'Azienda Zero, recepito dalla Regione Piemonte con D.G.R. n. 3-5267 del 28 giugno 2022;

- dato, altresì, atto che la citata L.R. n. 26/2021, art. 1 di modificazione della L.R. n. 18/2007 art. 23, comma 3, lett. d, ascrive ad Azienda Zero, tra le altre, le seguenti funzioni:

d) gestione e sviluppo del sistema informativo di telemedicina e di progetti ICT approvati dalla Giunta regionale, sentita la commissione consiliare competente, che ricoprono carattere di strategicità per la Regione… omissis";

- preso atto che Il Piano Nazionale di Ripresa e Resilienza ha previsto specifici obiettivi per la transizione digitale con particolare riferimento agli "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture Digitali" orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni;

- preso altresì che in questo contesto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica Amministrazione, si inserisce la creazione del Polo Strategico Nazionale, una nuova infrastruttura digitale a servizio della PA italiana, che la dota di tecnologie e infrastrutture cloud affidabili, resilienti e indipendenti;

- preso atto che in data 24 giugno 2022 il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri e la Società Polo Strategico Nazionale S.p.A ("PSN S.p.A.") con sede legale in Roma, via Goito 4, C.F. e Partita IVA 1682525100, hanno sottoscritto una convenzione, ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del D.lgs. 18 aprile 2016, n. 50 avente ad oggetto la concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012 CIG di convenzione 9066973ECE;

- preso atto che entro 32 mesi dalla data di stipula della convenzione le Amministrazioni interessate possono aderire alla convenzione mediante la stipula dei contratti di utenza, con durata massima di dieci anni ed effettuare la migrazione dei dati, servizi e applicazioni;

- atteso che Azienda Zero ha l'obiettivo di governare e monitorare nel tempo l'intero ciclo di vita tecnico- amministrativo degli applicativi gestionali in uso da ospitare sull'infrastruttura del PSN;

- Cred.NET
- DB Oracle
- ScrybaSign
- DocSuite;

- dato atto che, al fine di aderire alla convenzione sopra richiamata, Azienda Zero con PEC prot. n. 1084 del 04/05/2023, ha trasmesso al Concessionario il proprio Piano dei fabbisogni, allegato al presente provvedimento quale parte integrante e sostanziale, richiedendo la formulazione di un progetto tecnico economico per le necessità esposte.

- dato atto che con PEC acquisita al protocollo aziendale di Azienda Zero n. 4003/2023 del

2.10.2023, il concessionario ha presentato il Progetto del Piano dei Fabbisogni (Piano Operativo), allegato al presente atto quale parte integrante e sostanziale e la relativa proposta tecnico economica.

- dato atto che a seguito della approvazione del Progetto del Piano dei Fabbisogni (Piano Operativo) sopra richiamato, verrà stipulato con la società Polo Strategico Nazionale con sede legale in Roma, via Goito 4, numero di iscrizione nel Registro delle Imprese di Roma 1678264, C.F. e Partita IVA 1682525100, il contratto di utenza conforme allo schema allegato al presente atto quale parte integrante e sostanziale;

- valutato che l'importo presunto complessivo relativo ai 5 (cinque) anni di vigenza contrattuale ammonta complessivamente a euro 300.219 IVA esclusa, pari ad euro 366.267,18 IVA compresa verrà iscritto al bilancio di Azienda Zero al conto 03.10.05.03, "Canoni per beni strumentali non sanitari" secondo il piano dei costi di seguito riportato:

Anno 2023 : 27.317 IVA esclusa, pari ad euro 33.326,74 IVA inclusa
Anno 2024 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
Anno 2025 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
Anno 2026 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
Anno 2027 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
Anno 2028 : 50.529 IVA esclusa, pari ad euro 61.645,38 IVA inclusa

- ritenuto per quanto sopra esplicitato di proporre l'adesione alla convenzione avente ad oggetto la concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione, denominata Polo Strategico Nazionale (PSN).

- vista la disponibilità dell'Ing. Salvatore Scaramuzzino, direttore f.f. della SC Sistema Informativo di Azienda Zero, ad essere nominato Responsabile Unico di Progetto (RUP) e dell'art. 15 del D.lgs. n. 36/2023;

- acquisita la proposta del Responsabile Unico di Progetto, di nominare il dott. Luca Ghio, Collaboratore Tecnico Professionale Informatico in regime di convenzione presso Azienda Zero, quale Direttore Esecutivo del Contratto (DEC) ai sensi dell'art. 114, comma 8, del D.lgs. n. 36/2023;

- dato atto che alla data di adozione del presente provvedimento non risultano attribuiti ai singoli ordinatori di spesa i relativi budget e che, pertanto, il provvedimento va assunto con atto deliberativo e non già con determina dirigenziale;

Tutto ciò premesso:

IL COMMISSARIO
Dott. Carlo PICCO

nominato con D.G.R. n. 32-4847 del 31/03/2022

- visto il D. Lgs. 30.12.1992 n. 502 e successive modificazioni e integrazioni;
- vista la L.R. 24.01.1995, n. 10;
- vista la L.R. 6.08.2007, n. 18;
- esaminata e condivisa la succitata proposta del Direttore f.f. S.C. Sistema Informativo, ing. Salvatore Scaramuzzino;
- acquisito il parere favorevole espresso dal Direttore Amministrativo, dott. Alessandro Mazzantini e dal Direttore Sanitario, dott. Gianluca Ghiselli, a norma dell'art. 3 del D.lgs. 30.12.1992 n. 502, e successive modificazioni e integrazioni.

D E L I B E R A

1. di autorizzare l'adesione alla convenzione avente ad oggetto la concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione, denominata Polo Strategico Nazionale (PSN). della durata di 60 mesi, per un valore totale di euro 300.219 IVA esclusa, pari ad euro 366.267,18 IVA inclusa, CIG derivato per la presente gestione procedurale A018A3E796;

2. di approvare il Piano dei Fabbisogni predisposto dalla S.C. Sistema Informativo, allegato al presente provvedimento quale parte integrante e sostanziale;

3. di approvare il progetto dei Fabbisogni (Piano Operativo), allegato al presente provvedimento quale parte integrante e sostanziale;

4. di dare dato atto che la spesa quantificata in euro 27.317 IVA esclusa, pari ad euro 33.326,74 IVA inclusa , IVA esclusa, sarà iscritta al bilancio di Azienda Zero al conto 03.10.05.03, "Canoni per beni strumentali non sanitari" per l'annualità 2023;

5. Di riservarsi di iscrivere gli importi di seguito dettagliati nei successivi bilanci di Azienda Zero:

   Anno 2024 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
   Anno 2025 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
   Anno 2026 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
   Anno 2027 : 55.019 IVA esclusa, pari ad euro 67.123,18 IVA inclusa
   Anno 2028 : 50.529 IVA esclusa, pari ad euro 61.645,38 IVA inclusa

6. di nominare quale Responsabile Unico di Progetto (RUP), ai sensi dell'art. 15 del D.lgs. n. 36/2023, l'ing. Salvatore Scaramuzzino, Direttore f.f. della SC Sistema Informativo di Azienda Zero;

7. di nominare, su proposta del Responsabile Unico di Progetto il dott. Luca Ghio, Collaboratore Tecnico Professionale Informatico in regime di convenzione presso Azienda Zero, quale Direttore Esecutivo del Contratto (DEC) ai sensi dell'art. 114, comma 8, del D.lgs. n. 36/2023;

8. di trasmettere il presente provvedimento per i controlli di competenza al Collegio Sindacale ai sensi dell'art. 14 della L.R. 24.01.1995 n. 10;

Allegati: n.1 Piano dei Fabbisogni;
n.1 Piano Operativo.

Firmatari:

Proponente: Ing. Salvatore Scaramuzzino

Responsabile del Procedimento: Ing. Salvatore Scaramuzzino

Direttore Amministrativo: Dott. Alessandro Mazzantini

Direttore Sanitario: Dott. Gianluca Ghiselli

Commissario: Dott. Carlo Picco

Estensore dell'atto: Ing. Salvatore Scaramuzzino

*I pareri favorevoli dei Direttori Amministrativo e Sanitario sono confermati con la sottoscrizione digitale del presente atto ed il rinvio automatico ai motivi della proposta. **I pareri sfavorevoli sono esplicitamente motivati ed indicati in un allegato, firmato digitalmente.**

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

F9-48-30-26-BB-E3-D2-B1-EF-A9-DA-F4-61-51-87-7B-73-C3-50-DA

CAdES 1 di 4 del 13/10/2023 12:31:50

Soggetto: Carlo Picco PCCCRL60E17L013P

Validità certificato dal 15/07/2022 13:20:59 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC46

CAdES 2 di 4 del 12/10/2023 15:51:49

Soggetto: Gianluca Ghiselli GHSGLC63C13L833N

Validità certificato dal 15/07/2022 13:40:29 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC90

CAdES 3 di 4 del 12/10/2023 15:48:16

Soggetto: Alessandro Mazzantini MZZLSN77A22G702G

Validità certificato dal 03/05/2023 13:54:17 al 03/05/2026 02:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT con S.N. 010D F350

CAdES 4 di 4 del 06/10/2023 17:23:35

Soggetto: SALVATORE SCARAMUZZINO SCRSVT86A01D976L

Validità certificato dal 20/09/2022 10:09:36 al 20/09/2025 10:09:36

Rilasciato da ArubaPEC EU Qualified Certificates CA G1, ArubaPEC S.p.A., IT con S.N. 77DE 32CB EE

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.

TEMPLATE

PIANO DEI FABBISOGNI

Data: 22/11/2022

Template Piano dei Fabbisogni

Ed. 1 - ver. 1.0

Polo Strategico Nazionale

INDICE

LISTA DELLE TABELLE

1 PREMESSA

Il Piano Nazionale di Ripresa e Resilienza ha previsto specifici obiettivi per la transizione digitale con particolare riferimento agli "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture Digitali" orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni. Per promuovere l'innovazione digitale nella Pubblica Amministrazione, l'Agenzia per l'Italia Digitale ha attivato un piano complessivo di trasformazione e digitalizzazione, ponendo al centro del modello strategico la componente infrastrutturale (come descritto nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022) con l'obiettivo di governare la trasformazione digitale. Le direttrici evolutive della componente infrastrutturale sono rappresentata da:

- Sovranità digitale;
- Sicurezza, assicurare un presidio tecnologico e operativo in grado di garantire i più alti standard di sicurezza:
  - Fisica (e.g. disaster recovery, business continuity, controllo accessi, etc..);
  - Informatica (e.g. prevenzione e risposta attacchi cyber, data protection, identity access management, etc.);
- Innovazione, attraverso le migliori soluzioni tecnologiche per le infrastrutture data center, la connettività, le piattaforme e i servizi cloud, garantendo trasferimento tecnologico di esperienze e know how con i leader globali.

In questo contesto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce la creazione del Polo Strategico Nazionale, una nuova infrastruttura digitale a servizio della PA italiana, che la dota di tecnologie e infrastrutture cloud affidabili, resilienti e indipendenti.

L'Amministrazione Azienda Sanitaria Zero, di recente costituzione, non dispone attualmente di un'infrastruttura IT on premise o in cloud. L'Amministrazione ha l'esigenza di creare una nuova infrastruttura che ospiti le applicazioni funzionali alla sua attività. Di seguito le esigenze attualmente censite:

- Gestione credenziali (CRED.NET): applicativo per governare e monitorare nel tempo l'intero ciclo di vita tecnico-amministrativo delle credenziali utente, dalla richiesta, all'assegnazione, alla scadenza sino alla revoca delle utenze del Sistema Informativo Aziendale
- Ambiente gestito per ospitare un database Oracle di circa 60 Gb utilizzato solo in consultazione
- Scryba Sign: applicazione centralizzata aziendale per gestire il DB dei firmatari e i relativi poteri di firma
- Docsuite: soluzione per la gestione documentale, protocollo e PEC
- Active Directory, inclusa possibilità di sincronizzazione con Azure AD
- VM ad uso cliente per installazione di software vari.

Si richiede un'infrastruttura opportunamente sovradimensionata per ospitare anche esigenze future non ancora censite (all'incirca il doppio della richiesta attuale).

2 DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Nelle seguenti tabelle si riportano i dati anagrafici dell'Amministrazione contraente e del suo referente.

Ragione sociale Contraente	
Ragione sociale	AZIENDA SANITARIA ZERO
Codice Fiscale	0000012685160017
Partita Iva	12685160017
Indirizzo sede legale	Via San Secondo, 29 bis
CAP	10128
Comune	Torino
Provincia	Torino
Cognome referente Contratto Esecutivo	Scaramuzzino
Nome referente Contratto Esecutivo	Salvatore
Indirizzo mail referente Contratto Esecutivo	salvatore.scaramuzzino@aziendazero.piemonte.it
PEC Amministrazione	protocollo@pec.aziendazero.piemonte.it

Tabella 1: Dati anagrafici dell'Amministrazione contraente

Riferimento referente tecnico	
Cognome	Scaramuzzino
Nome	Salvatore
Telefono fisso	
Cellulare	+39 3667148010
Indirizzo mail	salvatore.scaramuzzino@aziendazero.piemonte.it

Tabella 2: Dati anagrafici del referente tecnico

Data	Firma
30/06/2023	**Salvatore Scaramuzzino**

3 DOCUMENTI DI RIFERIMENTO

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022	CONVENZIONE ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l'affidamento in concessione dei servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili - "Polo Strategico Nazionale"
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato A)	Capitolato Tecnico e relativi annessi – Capitolato Servizi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato B)	"Offerta Tecnica" e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato C)	"Offerta economica del Fornitore – Catalogo dei Servizi" e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato D)	Schema di Contratto di Utenza
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato H)	Indicatori di Qualità
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato I)	Flussi informativi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato L)	Elenco dei Servizi Core, no Core e CSP

Tabella 3: Documenti di riferimento

3.1 DOCUMENTI APPLICABILI

Riferimento	Codice	Titolo
Template Piano dei Fabbisogni	PSN- TMPL- PNDF	Piano dei Fabbisogni Template

3.2 ACRONIMI

Acronimo	Descrizione
AI	Artificial Intelligence

CaaS	Container as a Service
CMP	Cloud Management Platform
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
VM	Virtual Machine

4 DEFINIZIONI

- ACN: l'Agenzia per la cybersicurezza nazionale, di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;
- DTD: il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri;
- Amministrazioni: le amministrazioni individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
- Dati dell'amministrazione: le informazioni trattate dall'amministrazione, o da terzi per conto dell'amministrazione;
- Regolamento: il Regolamento di cui all'articolo 33-septies, comma 4, del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante "livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione", adottato dall'Agenzia per l'Italia digitale (AgID), d'intesa con il DTD, con Determinazione n. 628/2021 del 15 dicembre 2021;
- Servizi dell'amministrazione: servizi erogati verso terzi o internamente all'amministrazione;
- "modalità A - trasferimento in sicurezza dell'infrastruttura IT": migrazione verso il cloud effettuata secondo la strategia di migrazione Lift&Shift (anche detta Rehost), ovvero la migrazione dell'intero servizio dell'amministrazione, comprensivo di applicazioni e dati su un hosting cloud senza apportare modifiche agli applicativi, ovvero replicando il servizio esistente in un ambiente cloud;
- "modalità B - aggiornamento in sicurezza di applicazioni in cloud": migrazione verso il cloud effettuata secondo le seguenti strategie:
  - *repurchase/replace*: si intende la migrazione del servizio dell'amministrazione verso una soluzione nativa in cloud, in genere erogata in modalità Software as a Service;
  - *replatform*: si intende la riorganizzazione dell'architettura applicativa sostituendo intere componenti del servizio in favore di soluzioni Cloud native in modo da usufruire dei benefici dell'infrastruttura Cloud;
  - *re-architect*: ha come obiettivo quello di ripensare significativamente l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare appieno i servizi cloud-native offerti dai cloud service provider per massimizzare i benefici che ne derivano;
- Housing: utilizzo delle infrastrutture impiantistiche e di connettività dei Data Center del PSN, dove verranno ospitate apparecchiature delle Amministrazioni;
- Hosting: utilizzo delle infrastrutture IT dei Data Center del PSN, dove verranno installate le componenti software e middleware delle Amministrazioni.

5 PIANO DI MIGRAZIONE

Il presente capitolo rappresenta il piano di migrazione al cloud di dati e servizi dell'Amministrazione, in linea con quanto richiesto nella determina del 7 ottobre 2022 del Dipartimento per la trasformazione digitale.

I servizi da portare su PSN sono:

- CRED.NET (applicativo per gestione credenziali utente)
- DB Oracle
- Scryba Sign
- Docsuite

5.1 Obiettivi

Servizio dell'amministrazione	Tipo di Migrazione
CRED.NET	modalità A - trasferimento in sicurezza dell'infrastruttura IT
DB Oracle	modalità A - trasferimento in sicurezza dell'infrastruttura IT
Scryba Sign	modalità A - trasferimento in sicurezza dell'infrastruttura IT
Docsuite	modalità A - trasferimento in sicurezza dell'infrastruttura IT

5.1.1 Descrizione Servizio CRED.NET

L'applicativo CRED.NET che si intende portare sul PSN consente di gestire la richiesta e la revoca delle credenziali degli utenti che le utilizzeranno, alimentando un archivio da utilizzare per la verifica periodica delle credenziali stesse.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata, conosciuta solamente al medesimo.
Il trattamento dei dati personali con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

- Autenticazione informatica
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Aggiornamento almeno annuale dell'individuazione dell'ambito del trattamento consentito ai soli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici

L'applicativo assolve ai punti sopra evidenziati, consentendo di gestire la richiesta e la revoca delle credenziali alimentando un archivio da utilizzare per la verifica periodica delle credenziali stesse.

La metodologia tecnica è quella Web Server.

5.1.2 Descrizione Servizio DB Oracle

L'Amministrazione ha necessità di caricare su un ambiente gestito (PaaS o DBaaS) un dump Oracle di circa 60 GB, in modo da poter effettuare esclusivamente query (non si tratta di un DB in produzione).

5.1.3 Descrizione Servizio Scryba Sign

ScrybaSign è la soluzione di Medas per la gestione unica aziendale di tutti gli aspetti legati alla sottoscrizione e validazione temporale di documenti digitali.

ScrybaSign, integrandosi con gli applicativi aziendali, fornisce loro servizi per la validazione dei documenti attraverso l'apposizione di tutte le tipologie di firma digitale (tradizionale e remota, automatica e interattiva) o di firma elettronica avanzata (grafometrica e PKI), nei diversi formati (PAdES, CAdES, XAdES). Offre inoltre una soluzione di Firma Digitale Remota Semplificata, approvata specificamente da AgID, che consente di apporre firme digitali con l'uso della sola password di firma, senza OTP né relativi token.

ScrybaSign consente la gestione dell'intero ciclo di vita dei certificati di firma digitale ed elettronica avanzata: emissione, sospensione, riattivazione, revoca e rinnovo secondo tempistiche configurabili.

ScrybaSign permette di definire in modo granulare l'abilitazione degli operatori alla firma o marcatura dei documenti in base alla loro tipologia e provenienza; garantendone la sottoscrizione solo da parte di soggetti autorizzati.

5.1.4 Descrizione Docsuite

Docsuite è la soluzione per la PA progettata per gestire, in modo totalmente digitale, la produzione e gestione di documenti e procedimenti amministrativi, dalla creazione o inserimento fino all'archiviazione dei documenti, in conformità alle normative. Completamente web based e modulare, include le funzionalità e le potenzialità di un sistema di gestione documentale e di un motore di workflow consentendo di interfacciarsi con altri sistemi informatici in uso alla PA.
Aiuta ad assolvere gli obblighi di trasparenza e anticorruzione e facilita e lo scambio collaborativo di informazioni e documentazione.
DocSuite soddisfa i requisiti di registrazione a normativa del Protocollo Informatico. La registrazione dei documenti ricevuti include PEC, PosteWeb ed email, ed è agevolata la gestione dell'archivio ibrido digitale e cartaceo.
La gestione del flusso di adozione degli atti è completamente digitalizzata. Include nativamente gli strumenti per guidare in modo sicuro l'utente all'assolvimento di tutti gli obblighi pubblicistici, di trasparenza e anticorruzione previsti dalla normativa vigente. La gestione dei rapporti con gli organi di vigilanza è integrata nel flusso degli atti.

5.2 Piano di migrazione

Nome servizio	Classificazione dei Dati	Tipo di migrazione	Budget – Costi di migrazione	Budget - Canone annuale	Previsione tempi Migrazione
CRED.NET	Ordinari	Modalità A	Da definire	Da definire	3 mesi
DB Oracle	Ordinari	Modalità A	Da definire	Da definire	3 mesi
Scryba Sign	Ordinari	Modalità A	Da definire	Da definire	3 mesi
Docsuite	Ordinari	Modalità A	Da definire	Da definire	3 mesi

5.2.1 Tempistiche

Si riportano di seguito le tempistiche per gli ambienti da migrare:

Nome servizio	T1 Analisi & Discovery	T2 Setup	T3 Migrazione	T4 Collaudo
CRED.NET	T0 + 10 giorni	T1 + 5 giorni	T2 + 1 giorni	T3 + 1 giorni
DB Oracle	T0 + 10 giorni	T1 + 5 giorni	T2 + 1 giorni	T3 + 1 giorni
Scryba Sign	T0 + 10 giorni	T1 + 5 giorni	T2 + 1 giorni	T3 + 1 giorni
Docsuite	T0 + 30 giorni	T1 + 10 giorni	T2 + 1 giorni	T3 + 1 giorni

6 DESCRIZIONE DEI FABBISOGNI

6.1 Contesto di Riferimento

L'Amministrazione non ha attualmente un'infrastruttura on premise. Di seguito si riporta una bozza delle risorse richieste:

Applicativo	Descrizione	vCPU	RAM	Disco totale	SO	Middleware	Backup
CRED.NET		4	16	100	Centos		200
Dump DB Oracle		2	16	60		Oracle Std	120
Scryba Sign		4	8	120	Linux Ubuntu 16.04 LTS		240
		2	4	40	Linux Ubuntu 16.04 LTS		80
Docsuite	Front-end	4	8	208	Windows Server 2019		416
	Back-end	8	16	208	Windows Server 2019		416
	RDBMS	4	16	648	Windows Server 2019	SQL 2019 Std	1296
	Stampa conforme	2	8	208	Windows Server 2019		416
	Dgroove Ingestor 1	4	8	1000	Linux Ubuntu 22.04 LTS		2000
	Dgroove Ingestor 1	4	8	1000	Linux Ubuntu 22.04 LTS		2000
Generico	VM Generica	2	8	250	Windows Server 2019		500
Active Directory	AD	2	8	100	Windows Server 2019		200
	AD Connect	4	8	250	Windows Server 2019		500
VPN Collector	Pfsense	2	4	50	Free BSD		100
	Totale IaaS	**42**	**104**	**4242**			**8484**

7 Servizi richiesti

SERVIZIO	Richiesto	Ipotesi Budget (€)
Industry standard – Hosting		
Industry standard - Housing		
Industry standard – IaaS	X	
Industry standard – PaaS	X	
Industry standard – CaaS		
Hybrid Cloud on PSN site		
Secure Public Cloud on Microsoft Azure		
Secure Public Cloud on Google GCP		
Public Cloud PSN Managed		
Servizi di migrazione	X	
Servizi professionali - Servizio Re-Architect		
Servizi professionali - Servizio Re-Platform		
Servizi professionali - Security Professional Services		
Servizi professionali - IT Infrastructure - Service Operations	x	
Servizi professionali - Business and culture enablement		
Altri servizi a listino>		

Tabella 4: Servizi richiesti: quadro di sintesi

7.1 Industry standard

7.1.1 IaaS

Il servizio IaaS consiste nel rendere disponibile delle risorse infrastrutturali virtualizzate ed è suddiviso in IaaS Private e IaaS Shared:

IaaS Private

- Infrastruttura virtualizzata e dedicata;
- Server fisici con a bordo il virtualizzatore Vmware su cui possono essere attivate solamente VM della Amministrazione (cluster dedicato);

IaaS Shared

- Porzione di infrastruttura virtualizzata all'interno di una piattaforma condivisa;
- Si acquisista un pool di risorse virtuali (vCPU, vGB di RAM, vGB di Storage) e il PSN è responsabile della gestione completa dell'infrastruttura sottesa, comprensiva degli strumenti di automation e orchestration.

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
IaaS Private (HA)	Blade Medium	24	256				Server features 2 socket Intel® Xeon® Scalable processor family, with up to 32 DIMMs (up to 6TB), PCIExpress® (PCIe) 4.0 enabled I/O slots, and 2 high bandwidth Ethernet and Fiber Channel mezzanine card. All Ethernet interfaces are 10/25Gbps, fully redundant, with jumbo frame enabled end to end in the overall infrastructure. All FC interfaces are 32Gbps. Sistema operativo escluso		
IaaS Private (HA)	Blade Large	36	768				Server features 2 socket Intel® Xeon® Scalable processor family, with up to 32 DIMMs (up to 6TB), PCIExpress® (PCIe) 4.0 enabled I/O slots, and 2 high bandwidth Ethernet and Fiber Channel mezzanine card. All Ethernet interfaces are 10/25Gbps, fully redundant, with jumbo frame enabled end to end in the overall infrastructure. All FC interfaces are 32Gbps. Processore Intel 6354, 18 core, 3.0GHz, cache 39MB, 205W. Sistema operativo escluso		
IaaS - Storage (HA)	Storage High Performance					500	SAN NVMe based, replicato intra-region, 170K IOPS per Storage Array	20	120
IaaS - Storage (HA)	Storage Standard Performance					500	SAN All Flash based, replicato intra-region, 130K IOPS per Storage Array		
IaaS - Storage (HA)	NAS					500	NVMe based, replicato intra-region, 130K IOPS per Storage Array		
IaaS - Storage (HA)	Object storage					500	Replicato inter-region		
IaaS - Storage (HA)	Storage HP Encrypted					500	SAN NVMe based, replicato intra-region, crittografato a livello di singolo volume, 170K IOPS per Storage Array		
IaaS - Storage (HA)	Storage SP Encrypted					500	SAN All Flash based, replicato intra-region, crittografato a livello di singolo volume, 130K IOPS per Storage Array		
IaaS Shared (HA)	VM Tiny			1	2	100			

IaaS Shared (HA)	VM Small			2	4	100	Replica intra-region sincrona con duplicazione delle risorse sul secondario (0<RPO<1min, 0<RTO (IaaS)<30min); include i costi del backbone con latenza <5ms; Gestione hypervisor, over-commit 1:2 Sistema operativo escluso Infrastruttura basata su server Intel 6342, 24 core, cache 36MB, 230W		
IaaS Shared (HA)	VM Medium			4	8	100			
IaaS Shared (HA)	VM Large			8	16	100			
IaaS Shared (HA)	VM X-Large			16	32	100			
IaaS Shared (HA)	Pool Small			8	32				
IaaS Shared (HA)	Pool Medium			16	64				
IaaS Shared (HA)	Pool Large			32	128				
IaaS Shared (HA)	Pool XLarge			64	256			1	120
IaaS Shared	VM Tiny			1	2	100	Gestione hypervisor, over-commit 1:2. Sistema operativo escluso		
IaaS Shared	VM Small			2	4	100			
IaaS Shared	VM Medium			4	8	100			
IaaS Shared	VM Large			8	16	100			
IaaS Shared	VM X-Large			16	32	100			
IaaS Shared	Pool Small			8	32				
IaaS Shared	Pool Medium			16	64				
IaaS Shared	Pool Large			32	128				
IaaS Shared	Pool XLarge			64	256				
IaaS Private	Blade Medium	24	256						
IaaS Private	Blade Large	36	768						
IaaS Shared (HA)	Pool - 1GB ram aggiuntivo				1		Risorsa aggiuntva per Pool IaaS shared		
IaaS Shared (HA)	Pool - 1vCPU aggiuntiva			1			Risorsa aggiuntva per Pool IaaS shared	20	120
IaaS Shared	Pool - 1GB ram aggiuntivo				1		Risorsa aggiuntva per Pool IaaS shared		
IaaS Shared	Pool - 1vCPU aggiuntiva			1			Risorsa aggiuntva per Pool IaaS shared		

Tabella 5: Fabbisogno IaaS

7.1.2 PaaS

Il servizio Industry Standard PaaS mette a disposizione una piattaforma in grado di erogare componenti di middleware secondo un modello a servizio (ad esempio Data Base) astraendo l'infrastruttura sottostante.
Il PSN è responsabile dell'infrastruttura sottostante comprensiva degli strumenti di automation e orchestration e si compone dei seguenti sottoservizi:

DBaaS

- Consente di configurare e gestire database utilizzando un servizio senza preoccuparsi dell'infrastruttura sottostante

IAM

- È un servizio di Identity Management applicativo che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano dentro il PSN

Big Data

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

Artificial Intelligence

- Mette a disposizione un set di algoritmi pre-addestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
PaaS - DB	Mysql			2			Licenza inclusa (ultima/penultima versione certificata). Servizio gestito.		
PaaS - DB	PostgreSQL			2			Licenza inclusa (ultima/penultima versione certificata). Servizio gestito.		
PaaS - DB	SQL server			2	8		Licenza inclusa (ultima/penultima versione certificata). Servizio gestito.	2	120
PaaS - DB	Oracle dbms - Enterprise			4	12		Servizio gestito (ultima/penultima versione certificata). Licenza Oracle Enterprise Edition inclusa.		
PaaS - DB	Oracle dbms - Standard			2	12		Servizio gestito (ultima/penultima versione certificata). Licenza Oracle Standard Edition inclusa.	1	120
PaaS - DB	MongoDB			2			Licenza inclusa (ultima/penultima versione certificata). Servizio gestito.		
PaaS - DB	MariaDB			2			Licenza inclusa (ultima/penultima versione certificata). Servizio gestito.		
PaaS - Big Data	Data Lake - 1TB					1024	HDFS - ridondanza 3 copie - 20K IOPS		
PaaS - Big Data	Batch/Real time Processing - 1 Worker			4	128		Apache Spark su processore fisico 26 core 2,70 Ghz con virtualization ratio 1:2		
PaaS - Big Data	Event Message - 1 Worker			4	32		Apache Kafka su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2		
PaaS - Big Data	Data Governance						Portale self-service con catalogo e governance dei dati		
PaaS - AI	AI Platform - 1 Worker - 1 GPU			8	64		Spark/Tensorflow/Keras/scikit processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 - Nvidia A100 dedicata		
PaaS - AI	Semantic Knowledge Search - 1 Worker			8	32	2046	ElasticSearch su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2 - Disco SSD		
PaaS - AI	Text Analytics /NLP - 1 Worker			8	32		Analisi linguistica con entity recogniction, sentiment analysis, NER su processore fisico 26 core 2,70 Ghz virtualization ratio 1:2		
PaaS - AI	Audio Analytics - 1 flusso audio H24 X 365G						Analisi audio per speech to text, text to speech,speaker verification, speaker identification, anomaly detection		
PaaS - AI	Video Analytics - 1 flusso video H24 X 365G						Analisi video per object recogniction, object tracking, face recogniction, crowd counting		
PaaS - Spid Enabling & Profiling	Spid Enabling & Profiling 100 Utenti								

Tabella 6: Fabbisogno PaaS

7.2 Servizio di migrazione

Servizio di migrazione end-to-end chiavi in mano sia fisica (housing) che virtuale (dall'analisi degli applicativi al test sui nuovi ambienti e messa in produzione) dell'infrastruttura IT dell'Amministrazione verso l'infrastruttura PSN.

Le figure professionali saranno quantificate in fase di redazione del Progetto del Piano dei Fabbisogni.

7.3 Servizi professionali

L'Amministrazione richiede i seguenti ulteriori servizi professionali:

- IT Infrastructure - Service Operations

Le figure professionali saranno quantificate in fase di redazione del Progetto del Piano dei Fabbisogni.

7.3.1 IT Infrastructure - Service Operations

Servizi specialistici on demand a supporto delle Operations per la gestione dell'infrastruttura e del parco applicativo cliente.

7.4 Altri servizi a listino

La tabella riporta ulteriori servizi opzionali attivabili:

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
Sistemi operativi	Windows Server STD CORE (2 core)						Licenza Microsoft Server. Ultima release disponibile	18	120
Sistemi operativi	Red Hat per VM						Licenza Red Hat per singola VM. Ultima release disponibile.		
Sistemi operativi	Red Hat per Bare Metal						Licenza per due socket. Ultima release disponibile.		
Data Protection	Opzione DR						Replica su altra region		
Data Protection	Backup					1.000	Gestione delle policy in modalità self-managed; cifratura dei dati; ripristino granulare dei dati in modalità "a caldo e out-of-place"; seconda copia intra-region; GDPR compliant	20	120
Data Protection	Golden copy					1.000	Protezione antivirus, antimalware e anti-ramsonware proattivo; WORM copy; archiviazione in ambiente protetto privo di ogni accesso fisico e logico		
Multicloud	CMP per server						Portale self-service con catalogo dei servizi unificato; Governance; Dashboard personalizzabile; Capacity Planning; Compliance; Report di Cost Control e Capacity planning and Resource Usage; Performance Monitoring; Gestione finanziaria dell'IT		
Security	Antivirus						Prezzo per istanza		
Connettività	Connessione dedicata 1 Gbps						Tecnologia Gbe MPLS, profilo Silver 1000, TIR L2/L3 e outsourcing		

Tabella 7: Fabbisogno altri servizi a listino

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

E4-33-D8-7C-95-7A-7F-9F-40-3E-AE-81-9B-AA-20-B7-DF-D1-46-FB

CAdES 1 di 4 del 13/10/2023 12:31:51

Soggetto: Carlo Picco PCCCRL60E17L013P

Validità certificato dal 15/07/2022 13:20:59 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC46

CAdES 2 di 4 del 12/10/2023 15:51:49

Soggetto: Gianluca Ghiselli GHSGLC63C13L833N

Validità certificato dal 15/07/2022 13:40:29 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC90

CAdES 3 di 4 del 12/10/2023 15:48:17

Soggetto: Alessandro Mazzantini MZZLSN77A22G702G

Validità certificato dal 03/05/2023 13:54:17 al 03/05/2026 02:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT con S.N. 010D F350

CAdES 4 di 4 del 04/07/2023 08:09:43

Soggetto: SALVATORE SCARAMUZZINO SCRSVT86A01D976L

Validità certificato dal 20/09/2022 10:09:36 al 20/09/2025 10:09:36

Rilasciato da ArubaPEC EU Qualified Certificates CA G1, ArubaPEC S.p.A., IT con S.N. 77DE 32CB EE

Polo Strategico Nazionale

Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 29/09/2023 11:32
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

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

CUP: J51B21005710007

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

Azienda Sanitaria Zero

Polo Strategico Nazionale

SOMMARIO

Polo Strategico Nazionale

Indice delle tabelle

Polo Strategico Nazionale

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Prima Emissione	1	19/09/2023

Tabella 1: Informazioni Documento

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

Tabella 2: Autore

Revisione:	
PSN Solution team	n.a.

Tabella 3: Revisore

Approvazione:	
PSN Solution team	Paolo Trevisan
PSN Commercial team	Riccardo Rossi

Tabella 4: Approvatore

Polo Strategico Nazionale

LISTA DI DISTRIBUZIONE

INTERNA A:

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

ESTERNA A:

- Referente Contratto Esecutivo Azienda Sanitaria Zero
  - Salvatore Scaramuzzino
  - Email: salvatore.scaramuzzino@aziendazero.piemonte.it
- Referente Tecnico Azienda Sanitaria Zero
  - Salvatore Scaramuzzino
  - Email: salvatore.scaramuzzino@aziendazero.piemonte.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 dell'***Azienda Sanitaria Zero*** 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 **2023-0000012685160017-PdF-P1R1**).

Polo Strategico Nazionale

2 AMBITO

L'Amministrazione Azienda Sanitaria Zero, di recente costituzione, non dispone attualmente di un'infrastruttura IT on premise o in cloud. L'Amministrazione ha l'esigenza di creare una nuova infrastruttura che ospiti le applicazioni funzionali alla sua attività. Di seguito le esigenze attualmente censite:

- Gestione credenziali (CRED.NET): applicativo per governare e monitorare nel tempo l'intero ciclo di vita tecnico-amministrativo delle credenziali utente, dalla richiesta, all'assegnazione, alla scadenza sino alla revoca delle utenze del Sistema Informativo Aziendale
- Ambiente gestito dall'Amministrazione per ospitare un database Oracle di circa 60 Gb utilizzato per ospitare dump RMAN di Oracle on premise
- Scryba Sign: applicazione centralizzata aziendale per gestire il DB dei firmatari e i relativi poteri di firma
- Docsuite: soluzione per la gestione documentale, protocollo e PEC
- Active Directory, inclusa possibilità di sincronizzazione con Azure AD
- VM ad uso cliente per installazione di software vari.

Si richiede un'infrastruttura opportunamente sovradimensionata per ospitare anche esigenze future non ancora censite su infrastruttura IaaS.

La classificazione dei dati è di tipo ORDINARIO.

Si precisa che si tratta di nuovi servizi, per cui è prevista l'installazione ex novo.

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
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
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
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.

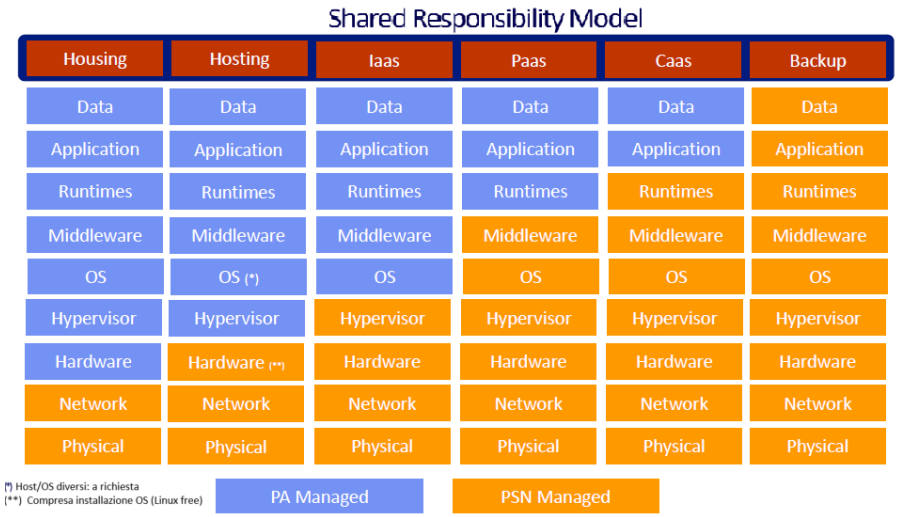
5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
Industry Standard	Housing
Industry Standard	Infrastructure as a Service (IaaS)
Industry Standard	Platform as a Service Database (PaaSDB)
Industry Standard	Data Protection: Backup
Industry Standard	Data Protection: Golden copy protetta
Servizi di Migrazione	
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:



5.2 INDUSTRY STANDARD

5.2.1 Housing

5.2.1.1 Descrizione del servizio

Il **Servizio Industry Standard Housing** è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di aree esclusive all'interno dei Data Center del PSN, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti descritti, atte ad ospitare le infrastrutture IT e TLC di proprietà dell'Amministrazione, nonché di eventuali variazioni in corso d'opera.

5.2.1.2 Personalizzazione del servizio

Sarà fornita all'Amministrazione una classe /29 di indirizzi IP pubblici.

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

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

5.2.1.4 Specifiche di collaudo

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

5.2.2 *Infrastructure as a Service*

5.2.2.1 *Descrizione del servizio*

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

Figura 1 Infrastructure as a Service

Il servizio IaaS è suddiviso in:

- **IaaS Private**: consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e dedicata, in grado di ospitare tutte le applicazioni in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica.

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

- **IaaS Shared:** consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e condivisa, in grado di ospitare tutte le applicazioni in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica.

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

5.2.2.2 *Personalizzazione del servizio*

La tabella seguente riporta il dimensionamento dei nuovi servizi richiesti dall'Amministrazione.

Applicativo	Descrizione	Servizio	vCPU	RAM (GB)	Disco totale (GB)	SO

CRED.NET		IaaS	4	16	100	Centos
Scryba Sign		IaaS	4	8	120	Linux Ubuntu 16.04 LTS
		IaaS	2	4	40	Linux Ubuntu 16.04 LTS
Docsuite	Front-end	IaaS	4	8	208	Windows Server 2019
	Back-end	IaaS	8	16	208	Windows Server 2019
	Stampa conforme	IaaS	2	8	208	Windows Server 2019
	Dgroove Ingestor 1	IaaS	4	8	1000	Linux Ubuntu 22.04 LTS
	Dgroove Ingestor 2	IaaS	4	8	1000	Linux Ubuntu 22.04 LTS
Generico	VM Generica	IaaS	2	8	250	Windows Server 2019
Active Directory	AD	IaaS	2	8	100	Windows Server 2019
	AD Connect	IaaS	4	8	250	Windows Server 2019
VPN Collector	Pfsense	IaaS	2	4	50	FreeBSD
	Totale IaaS		**42**	**104**	**3534**	

Tabella 10: Riepilogo risorse IaaS richieste dall'Amministrazione

Per rispondere alle esigenze è previsto un servizio **IaaS Shared HA** costituito da un Pool di Risorse vCPU, RAM e disco dimensionate per gestire una capacità aggiuntiva rispetto a quella prevista, considerata l'esigenza dell'Amministrazione di incrementare in tempi brevi i propri servizi.

La soluzione IaaS Shared HA consente di avere le risorse riallocabili sui due DC della stessa Region in caso di problematiche infrastrutturali su uno dei due DC.

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

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

5.2.2.4 Specifiche di collaudo

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

5.2.3 Platform as a Service

5.2.3.1 Descrizione del servizio

Il **Servizio Platform as a Service (PaaS)** è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad

esempio i Database, astraendo dall'infrastruttura sottostante. Il PSN, in qualità di provider, si fa carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

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

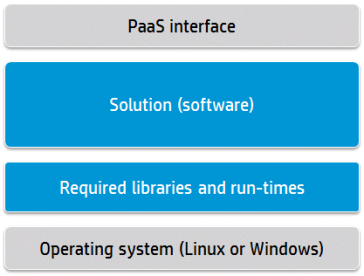


Figura 2 Platform as a Service

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

Il servizio PaaS si compone dei seguenti sottoservizi:

- **Database as a Service (DBaaS):** consente all' Amministrazione di configurare e gestire il database utilizzando un servizio senza preoccuparsi dell'infrastruttura sottostante. Il PSN è responsabile di tutto lo **stack d'infrastruttura** comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche;
- **Identity Access Management (IAM):** consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano nel PSN;
- **Big Data:** consente la costruzione di Data Lake as a Service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale;
- **Artificial Intelligence (AI):** mette a disposizione un set di algoritmi pre-addestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning.

5.2.3.2 Platform as a Service - Database

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

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

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

5.2.3.3 Personalizzazione del servizio

La tabella seguente riporta il dimensionamento dei nuovi servizi richiesti dall'Amministrazione.

Applicativo	Descrizione	Servizio	vCPU	RAM (GB)	Disco totale (GB)	Versione
Dump DB Oracle	DB Oracle	PaaS	2	16	60	Oracle Std Ed
Docsuite	DB SQL Server	PaaS	4	16	648	SQL Server 2019 Std Ed
	Totale PaaS		6	32	708	

Tabella 11: Riepilogo risorse PaaS richieste dall'Amministrazione

Per rispondere alle esigenze sono previsti due servizi **PaaS DB Oracle e SQL Server** con i dimensionamenti secondo specifiche dell'Amministrazione.

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

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

5.2.3.5 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.

5.2.4 Data Protection e Disaster Recovery

5.2.4.1 Data Protection: Backup

Servizio «self-managed» l'utente ha completa autonomia di gestione nella definizione della policy di backup ed il recupero degli stessi, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software. Il ripristino può avvenire ad una certa data in relazione alle copie di backup effettuate. Il servizio di backup standard prevede di effettuare il backup dello storage base (100GB) previsto per ogni istanza.
Per tutti i backup sarà effettuata una ulteriore copia secondaria al completamento della copia primaria presso il Data Center secondario.
Le principali caratteristiche del servizio che verrà realizzato sono:

- La possibilità di effettuare backup full e incrementali;
- Cifratura dei dati nella catena end to end (dal client alla libreria);
- Possibilità di organizzare i backup ed effettuare ricerche sulla base di differenti filtri (es. date di riferimento) e mantenere più backup in contemporanea;

- Possibilità di poter selezionare cartelle e file da sottoporre a backup e possibilità di escludere tipologie di file per nome, estensione e dimensione per i backup di tipo file system (con installazione di un agent sui server oggetto di backup);
- la conservazione e svecchiamento dei dati del back-up secondo policy di retention standard: 7 giorni, 1 mese, 2 mesi, 3 mesi, 6 mesi, 1 anno, 10 anni;
- possibilità di modificare la policy di retention (tra quelle su indicate) applicate ai backup;
- monitoring dei jobs di backup e restore;
- reportistica all'interno della console;
- un metodo efficiente per trasmissione ed archiviazione applicando tecniche di compattazione e compressione ed identificando ed eliminando i blocchi duplicati di dati durante i backup.
- Il ripristino dei dati scegliendo la versione dei dati da ripristinare in funzione della retention applicata agli stessi.
- il ripristino granulare dei dati (singolo file, mail, tabella, ecc.) in modalità "a caldo e out-ofplace" garantendo quindi la continuità operativa. Tale modalità di ripristino assicura la possibilità di effettuare dei test di restore in qualsiasi momento e con qualsiasi cadenza.
- Repository storage del servizio su apparati di tipo NAS o S3 (AWS-S3 compatibile)
- GDPR Compliant: Supporta utente e ruoli IAM oltre alla cifratura del dato e controllo degli accessi

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

5.2.4.2 Data Protection: Golden copy protetta

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, il PSN mette a disposizione un servizio opzionale aggiuntivo che analizza i backup mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione.
Si tratta di una funzionalità completamente gestita ed opzionale, attivabile su richiesta, in aggiunta al servizio di Backup standard: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy; in particolare, quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum e CRC per ogni blocco di dati sul sistema sorgente e queste *signature* vengono utilizzate per convalidare i dati del backup. Una volta validate, tali *signature* vengono memorizzate con il backup stesso: ciò permette di eseguire automaticamente la verifica della consistenza dei dati salvati nel backup, utilizzando le signature salvate.

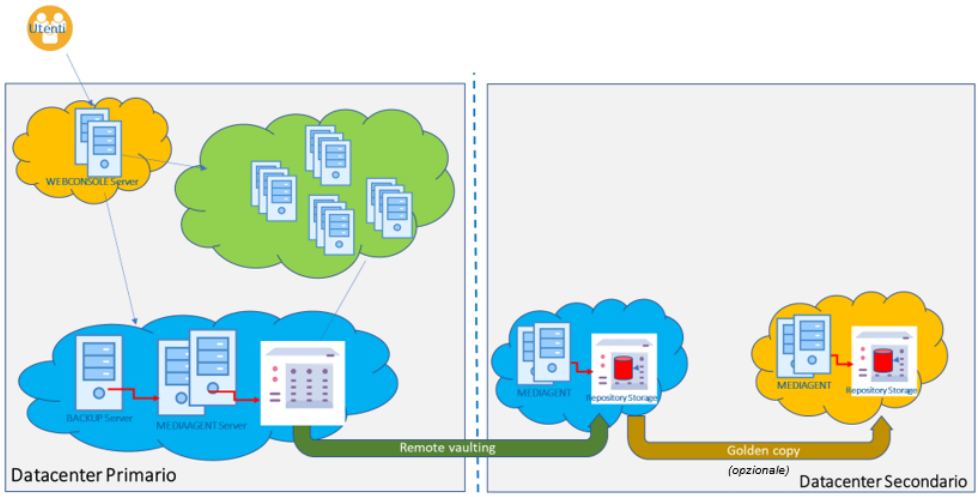


Figura 3 Architettura Funzionale Golden Copy

Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (*WORM: Write Once, Read Many*) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute, ecc) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.
Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).
Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali attacchi ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che, opportunamente gestiti, consentono di condizionare e inibire la creazione della golden copy.
Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo *ransomware* non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: Solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo *ransomware*, si potrà procedere all'archiviazione della "*golden copy*" in un ambiente protetto e in sola lettura.
Le principali caratteristiche del servizio sono:

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

5.2.4.3 Personalizzazione del servizio

Il dimensionamento del backup è stato fatto sulla base di una policy che prevede l'incrementale giornaliero, il full settimanale ed una retention pari a due settimane.

La policy adottata, considerando la doppia copia di backup prevista su due DC distinti, porta ad un dimensionamento annuo di c.a 29 TB per il backup e la Golden Copy.

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

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

5.2.4.5 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

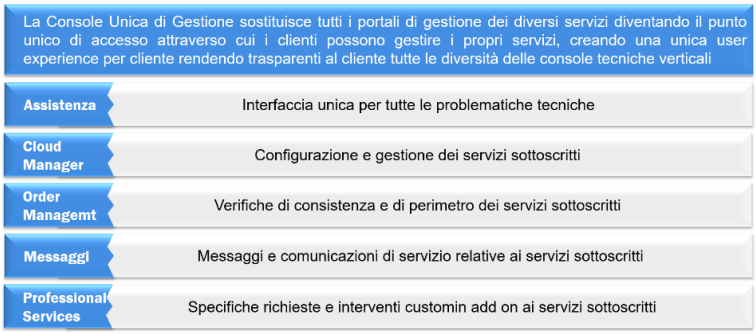


Figura 4 Funzionalità CU

delle risorse istanziate ma anche per definire un modello di IaC (Infrastructure as Code); segnalare eventuali anomalie in modalità "self".

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.

Polo Strategico Nazionale

5.3.2 Modalità di accesso

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

5.3.3 Interfaccia applicativa della Console Unica

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

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

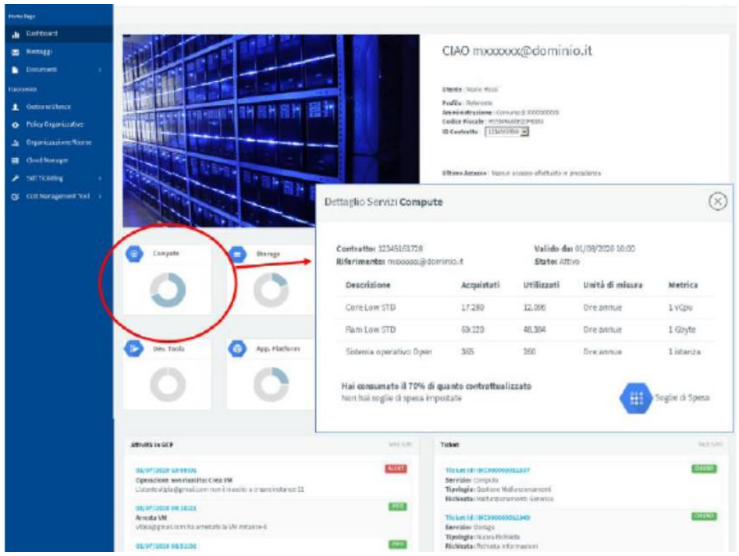


Figura 5 Dashboard CU

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

Dettagliando ulteriormente la sezione di Design & Delivery, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di definire e configurare le risorse cloud contrattualizzate in modalità semplificata

ed aderente ai requisiti e alla classificazione dei servizi della Convenzione, garantendo massima autonomia e tempestività nell'attivazione.
Il referente dell'Amministrazione, accedendo dalla sezione "I tuoi servizi" alla dashboard del Cloud Manager potrà nella fase di Design & Delivery:

- selezionare, utilizzando l'apposito menu a tendina presente nell'header della pagina, un Project tra quelli esistenti;
- visualizzare sia le categorie di servizio in cui sono state attivate risorse con il relativo dettaglio (identificativo della risorsa) sia quelle che non hanno risorse istanziate;
- istanziare in modo semplificato, per ciascuna categoria di servizi della Convenzione, attraverso la funzionalità "Configura", nuove risorse cloud utilizzando una procedura guidata che espone solo le funzionalità base per l'attivazione delle risorse cloud garantendo velocità di esecuzione. Nel caso in cui l'Amministrazione voglia, invece, utilizzare tutte le funzionalità di configurazione del Cloud Manager potrà accedervi direttamente dal tasto "Funzionalità Avanzate" presente in ciascuna finestra di configurazione.
- monitorare, in fase di attivazione delle risorse, lo stato di avanzamento dei consumi per la specifica categoria di servizi nel Project selezionato in modo da avere sempre a disposizione una vista delle quantità disponibili e in uso.

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

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

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

5.4 SERVIZI E PIANO DI MIGRAZIONE

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assessment effettuati in fase di definizione delle esigenze dell'Amministrazione, tenendo conto di eventuali vincoli temporali ed architetturali di dettaglio oltre che di specifiche esigenze di customizzazione.
Per l'intero periodo di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

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

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

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

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

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

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

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

Figura 6: Servizio di Migrazione - Metodologia EMG2C

Come già specificato, nel caso dell'Amministrazione non sono previste attività di migrazione, in quanto i servizi saranno installati ex novo.

Si riportano di seguito le fasi per il completamento del set up dell'infrastruttura.

1. **Set-up**

La fase è finalizzata a garantire un'efficace predisposizione dell'ambiente target su cui dovranno essere installati i servizi/applicazioni dell'Amministrazione e si articola nelle seguenti fasi:

- Progettazione operativa e di dettaglio.
- Predisposizione dell'infrastruttura target presso i DC del PSN.
- Predisposizione del networking e delle policy FW per la comunicazione tra DC e sede Cliente
- Installazione ex novo delle applicazioni

2. **Collaudo**

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

Esecuzione Collaudo: tale fase consiste nell'esecuzione dei test definiti in precedente e concordati con la Pubblica Amministrazione, per certificare il Go Live dell'applicazioni sull'ambiente target.

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

La matrice RACI che segue illustra i ruoli per le attività di set up.

Di seguito la descrizione dei 4 Ruoli:

(R) Responsible: Il Responsible svolge concretamente il lavoro. Ogni attività richiede almeno un Responsible.

(A) Accountable: l'Accountable è la persona o stakeholder che detiene l'ownership dell'attività, ovvero deve dare l'approvazione finale quando tale attività viene completata.

(C) Consulted: sono tutte quelle persone o parti interessate che hanno bisogno di dare un contributo prima che il lavoro possa essere svolto e approvato, ovvero forniscono informazioni e ci si aspetta una comunicazione bidirezionale.

(I) Informed: persone o parti interessate che devono essere tenute al corrente sullo stato di avanzamento dell'attività. Hanno bisogno di aggiornamenti sui progressi o sulle decisioni prese, ma non hanno bisogno di essere consultati formalmente, né contribuiscono direttamente all'attività o alla decisione.

Applicativo	Attività	PSN	Amministrazione
CRED.NET	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA
Dump DB Oracle	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA
Scryba Sign	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA

Docsuite	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA
Server Generico	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA
Active Directory	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	CI	RA
	Collaudo Applicativo	CI	RA
VPN Collector	Progettazione	RA	CI
	Predisposizione infrastruttura target	RA	CI
	Predisposizione networking	RA	CI
	Installazione applicazioni	RA	CI
	Collaudo Applicativo	RA	CI

Tabella 12: Matrice RACI set up e collaudo

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.

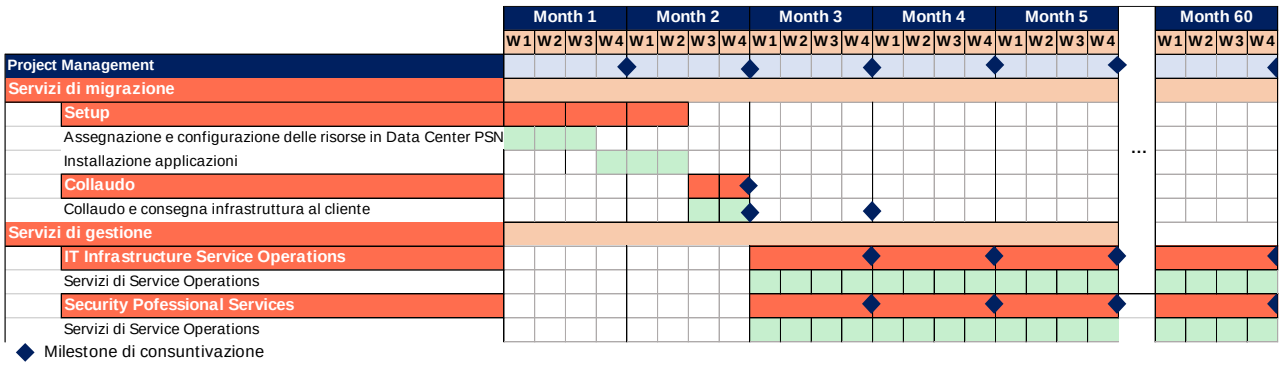


Tabella 13: GANTT

5.4.2 Security Profess. Services

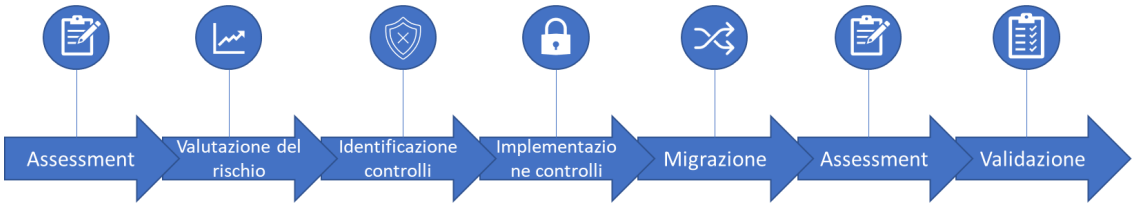
La migrazione su cloud è un processo complesso e un cambiamento rilevante che non va preso alla leggera. Non esiste una procedura di migrazione immediata sul cloud, e anzi spesso i rischi di migrazione stessi non vengono opportunamente valutati con il risultato che un'attività di migrazione che dovrebbe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

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

I servizi sono necessari per:

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

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



5.4.2.1 Security Professional Services - Cybersecurity Resilience and Readness

Alla luce delle crescenti minacce informatiche per le organizzazioni, garantire l'adeguato livello di protezione delle reti, dei dati e dei servizi, diventa un fattore di primaria importanza. Questo rappresenta un passaggio molto complesso in cui i rischi della migrazione spesso non vengono opportunamente valutati con l'effetto

di diminuire, invece che migliorare, il livello complessivo di sicurezza delle applicazioni, esponendo i workload migrati a nuove tipologie di 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.

Pertanto in linea con i principali standard normativi di riferimento nonché delle più efficaci capacità difensive attivabili nel breve/medio periodo da parte dell'Ente, vengono previste una serie di soluzioni di servizi orientati a migliorare la resilienza operativa mantenendo al contempo una visione in tempo reale del panorama delle minacce esistenti predisponendo reattivamente, piuttosto che proattivamente, le opportune risposte a tipologie di minacce specifiche piuttosto che incidenti operativi di sicurezza informatica impattanti l'operatività dell'Ente. Viene quindi predisposto il seguente *piano di attivazione* servizi cyber security. Di seguito brevemente i servizi previsti e descritti nel dettaglio in opportuni paragrafi:

- Assessment, valutazione dei rischi e delle vulnerabilità legate al processo di migrazione:
  - Vulnerability Assessment, Research & Exploitation;
  - Web Application Penetration Testing;
  - Dynamic Application Security Testing;
- Sicurezza hosts Antivirus (AV) - (EDR)

I servizi professionali saranno erogati a task con la modalità di remunerazione "a corpo" con una tariffa giornaliera fatturata a stato avanzamento lavori (mensile/bimestrale). Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente, nonché il corretto Team Mix di risorse. La fatturazione avverrà alla consegna dei deliverable concordati, previo benestare sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro.

Per quanto riguarda l'erogazione dei servizi di supporto, si precisa che la modalità di remunerazione di tali servizi è "a corpo" con una tariffa giornaliera fatturata a stato avanzamento lavori.

On top a tutti i servizi previsti viene fornito anche un supporto di *Service Assurance* finalizzato a supportare l'Amministrazione nelle seguenti attività:

- Focal point durante la fase di programmazione startup dei servizi cyber;
- Intercettare possibili criticità al fine di identificare le opportune azioni con gli attori coinvolti;
- Focal point per la condivisione delle nuove necessità dell'Amministrazione;
- Supervisionare la conduzione dei servizi previsti da contratto;
- Rappresenta un livello di escalation rispetto alle attività ordinarie
- Partecipare attivamente alle attività di Kick Off Meeting (KOM) con l'Amministrazione;

Polo Strategico Nazionale

5.4.2.2 Vulnerability Assessment, Research & Exploitation

Il servizio sarà erogato in modalità one shot da remoto e prevederà una fase preparatoria ed una fase operativa in funzione della soluzione target identificata con l'Amministrazione. Di seguito le attività che saranno erogate dal servizio:

- *Fase preparatoria*, redazione documentale: si procede alla redazione dei due documenti di Legal Agreement (LA) e di Rules Of Engagement (ROE).
- *Fase preparatoria*, raccolta di informazioni del perimetro di analisi (infrastruttura di rete, componenti hardware e software dei sistemi);
- *Fase Operativa*, individuazione delle vulnerabilità: tramite un set opportuno di strumenti automatizzati e correttamente configurati verrà collezionata una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati;
- *Fase Operativa*, classificazione delle vulnerabilità: le vulnerabilità individuate saranno classificate in funzione di livelli di priorità d'intervento secondo lo standard CVSS.

Nel dettaglio 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 definiscono il perimetro e modalità di esecuzione dei test sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test.

A valle dell'accettazione delle opportune manleve e regole di ingaggio partirà la *fase operativa*, di seguito le attività effettuate:

- esecuzione one shot di un Vulnerability Assessment sul perimetro di indirizzamento IP interno (o privato);
- analisi dei risultati;
- individuazione delle vulnerabilità attraverso l'esecuzione di test ad hoc che consentano di accertare l'impatto sui sistemi in analisi;
- assegnazione delle priorità/severità ai rischi di sicurezza in base al contesto;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);

Al completamento della *fase operativa*, saranno consegnati i seguenti deliverable:

- *VA Results Executive Summary* : Il report contiene una overview di tipo executive (ad alto livello) delle vulnerabilità individuate, ordinate per livello di rischio;
- *VA Results Technical Report*: Il report contiene i dettagli delle vulnerabilità segnalate, ordinate per criticità (utilizzando il sistema CVSS), incluse gli entry-point e le contromisure suggerite.

I deliverable, in base alla complessità del perimetro, possono far parte di un unico documento di report. Il servizio è limitato all'analisi di massimo qtà (50) IP.

5.4.2.3 Dynamic Application Security Testing

Il servizio sarà erogato in modalità one shot da remoto e consente l'identificazione delle vulnerabilità all'interno delle applicazioni Web e l'analisi dell'esposizione al rischio di attacchi informatici ai Sistemi Informativi mediante l'utilizzo di tecniche di analisi dinamica.

L'attività ha lo scopo di rilevare e gestire le vulnerabilità applicative che insistono sui sistemi informativi in ambiente WEB di produzione/pre-produzione e loro relative classificazione e prioritizzazione.

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.

Il servizio prevede l'esecuzione dei test dinamici di sicurezza per le applicazioni per la verifica delle vulnerabilità tenendo conto dell'esposizione e dell'ambiente operativo in cui l'applicazione è in esecuzione. L'input è rappresentato dalle informazioni relative ai target da analizzare e le relative modalità attuative che potranno essere concordate con

L'analisi comprenderà almeno i seguenti ambiti:

- Configurazione (es. directory traversing);
- Autenticazione (cifratura degli accessi, password policy, dictionary attack);
- Autorizzazione (Privilege escalation);
- Input Validation.

A seguito delle scansioni effettuate sarà prodotto un report indicante le vulnerabilità individuate e la relativa classificazione.

Il report costituirà il *Detailed Software Security Assessment Report* contenente i dettagli tecnici del livello di sicurezza dell'istanza a run-time applicazione:

- Riferimenti ai tipi di attacco e vulnerabilità
- Vulnerabilità/rischi identificati e la gravità di ognuno in termini di potenziale impatto sul sistema software oggetto dell'analisi
- Notazioni e classificazione dei bugs sulla sicurezza secondo gli standard applicabili

Il servizio è limitato all'analisi di massimo qtà 1 target (di max 30 url).

5.4.2.4 Servizio di Sicurezza hosts Antivirus (AV) - (EDR)

Nel presente paragrafo è descritto il servizio di Sicurezza hosts Antivirus (AV) - (EDR). L'attività è finalizzata alla protezione degli Endpoint identificati dall'Amministrazione secondo quanto di seguito rappresentato:

- Ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro (con agent installato);
- Mitigazione automatica (ove applicabile) per gli incidenti di sicurezza riconosciuti come "veri positivi" ed ad alta criticità;
- Garanzia della protezione degli Endpoint anche in assenza momentanea di connessione ad internet (in funzione del tipo di soluzione tecnologica prevista dall'Amministrazione);
- Possibilità di isolare dalla rete endpoint compromessi conservandone il controllo dalla piattaforma di management (in funzione del tipo di soluzione tecnologica prevista dall'Amministrazione);
- Protezione in tempo reale da attacchi sconosciuti e che non utilizzano metodologie e/o indicatori noti (limitatamente alle caratteristiche della soluzione tecnologica impiegata);

La gestione centralizzata della soluzione viene fatta attraverso una piattaforma di management che di fatto raccoglie tutte le informazioni di telemetria (metadati) inoltrate dagli agent installati sugli Endpoint dell'Amministrazione tramite opportuno collegamento Internet, subordinata alla visibilità continuativa necessaria fra agent e piattaforma di management (e non oggetto del presente servizio).

Il servizio è erogato as a service su un perimetro definito dall'Amministrazione ed include un monitoraggio continuativo con finestra di servizio H24 per 365 giorni, con notifica degli eventi ritenuti di interesse per l'Amministrazione attraverso un portale dedicato NGS, che garantisce discrezionalità nelle comunicazioni e negli accessi.

5.4.3 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.

5.4.3.1 Personalizzazione del servizio

In particolare, sono previste attività di supporto sistemistico per 5 anni a partire dalla data di collaudo, secondo quanto dettagliato nella seguente matrice RACI.

Di seguito la descrizione dei 4 Ruoli:

(R) Responsible: Il Responsible svolge concretamente il lavoro. Ogni attività richiede almeno un Responsible.

(A) Accountable: l'Accountable è la persona o stakeholder che detiene l'ownership dell'attività, ovvero deve dare l'approvazione finale quando tale attività viene completata.

(C) Consulted: sono tutte quelle persone o parti interessate che hanno bisogno di dare un contributo prima che il lavoro possa essere svolto e approvato, ovvero forniscono informazioni e ci si aspetta una comunicazione bidirezionale.

(I) Informed: persone o parti interessate che devono essere tenute al corrente sullo stato di avanzamento dell'attività. Hanno bisogno di aggiornamenti sui progressi o sulle decisioni prese, ma non hanno bisogno di essere consultati formalmente, né contribuiscono direttamente all'attività o alla decisione.

Nelle seguenti voci vi è la descrizione del campo "Tipologia supporto":

- Incluso: Attività inclusa nel canone di servizio
- Escluso: Attività non inclusa nel canone di servizio

Supporto Sistemistico

Finestra di copertura 8 x 5

Attività	Tipologia supporto	PSN	Amministrazione
OS Win/Lin - Gestione configurazioni di OS/applicativi	*Incluso*	RA	CI
OS Win/Lin – Configurazione, modifica, monitoring e troubleshooting backup e restore sistema operativo	*Incluso*	RA	CI
OS Win/Lin - Hardening e performance tuning	*Incluso*	RA	CI
OS Win/Lin - Gestione immagini per remote install/boot	*Incluso*	RA	CI
OS Win/Lin - IP Address Management	*Incluso*	RA	CI
OS Win/Lin - Asset inventory server	*Incluso*	RA	CI
OS Win/Lin - Deploy OS su virtual machines	*Incluso*	RA	CI
OS Win/Lin – Upgrade Sistema Operativo	*Incluso*	RA	CI
OS Win/Lin – Installazione Pack e Add-on aggiuntivi	*Incluso*	RA	CI
OS Win/Lin – Migrazione applicativa	*Escluso*	CI	RA
OS Win/Lin – gestione applicativa (Middleware)	*Escluso*	CI	RA
OS Win/Lin - Troubleshooting (Incident e Change management)	*Incluso*	RA	CI
OS Win/Lin - Patching OS con cadenza trimestrale (in accordo con i fornitori applicativi)	*Incluso*	RA	CI
OS Win/Lin - Creazione/gestione delle utenze, i privilegi e gli accessi ai sistemi	*Incluso*	RA	CI
OS Win/Lin - Gestione dei log di sistema e verifica delle eventuali irregolarità Nota: Eventuali licenze per software di log management sono a carico del cliente.	*Incluso*	RA	CI
OS Win/Lin – Gestione e installazione agenti di monitoraggio su OS	*Incluso*	RA	CI
OS Win/Lin - Monitoraggio dei parametri principali del server (CPU, RAM e spazio disco)	*Incluso*	RA	CI
OS Win/Lin – Condivisione eventuali parametri di monitoraggio avanzati (Servizi,Applicativi)	*Incluso*	CI	RA
OS Win/Lin – Scansione delle vulnerabilità con software OpenVAS e condivisione report	*Incluso*	RA	CI
vCloud – Gestione dell'ambiente IAAS	*Incluso*	RA	CI
Vcloud – Capacity Management	*Incluso*	RA	CI
Vcloud – Implementazione policy NSX (supporto a microsegmentazione, implementazione VPN)	*Incluso*	RA	CI
Vcloud – Gestione Load Balancer	*Incluso*	RA	CI
Consulenza su progetti evolutivi atti a migliorare la gestione e la sicurezza dell'ambiente del cliente	*Incluso*	RA	CI

Tabella 14: Matrice RACI Supporto Sistemistico

Si precisa che l'eventuale implementazione di Major change o di nuovi progetti non a perimetro che ridisegnino il design infrastrutturale potrà essere oggetto di successiva quotazione ad hoc.

Supporto DBA

Finestra di copertura 8 x 5

Attività	Tipologia supporto	PSN	Amministrazione
Monitoraggio disponibilità	*Incluso*	RA	CI
Gestione utenze e profili di database	*Incluso*	RA	CI
Gestione dei parametri d'istanza e di memoria	*Incluso*	RA	CI
Controllo periodico allocazione spazi per evitare blocchi applicativi	*Incluso*	RA	CI
Verifica dei log e tuning dei parametri d'istanza per il miglioramento e il mantenimento delle performance	*Incluso*	RA	CI
Verifica corretta schedulazione backup Nota: Richiede sottoscrizione Managed Backup Service	*Incluso*	RA	CI
Ricostruzione oggetti deframmentati (tabelle ed indici)	*Incluso*	RA	CI
Monitorare la crescita anomala di oggetti di database	*Incluso*	RA	CI
Segnalazione dell'esigenza dell'applicazione di patch o upgrade di release (da comunicare ai fornitori applicativi)	*Incluso*	RA	CI
Applicazione delle patch	*Incluso*	RA	CI
Upgrade di release	*Incluso*	RA	CI
Interventi di natura applicativa	*Escluso*	CI	RA

Tabella 15: Matrice RACI Supporto DBA

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.
- **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
- **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.
- **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
- **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.
- **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.

7 SICUREZZA

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

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

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

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

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

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

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

Polo Strategico Nazionale

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	0000012685160017
Ragione Sociale	Azienda Sanitaria Zero
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000012685160017-PdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	3.7

RIEPILOGO PREZZI				
SERVIZIO	Totale UT		Totale Canone Annuale	
Industry Standard			€	43.939,33
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	-
Public Cloud PSN Managed			€	-
Servizi di Migrazione	€	27.316,50		
Servizi Professionali	€	272.902,29		
TOTALE	€	300.218,79	€	43.939,33

Polo Strategico Nazionale

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	1			€ 65,4500
IAAS17	IndustrySt andard	IaaSSharedHA	Pool XLarge	1			€ 10.620,6400
IAAS03	IndustrySt andard	IaaSStorageHA	Storage High Performance	16			€ 5.824,8000
SO01	IndustrySt andard	SistemiOperativi	Windows Server STD CORE (2 core)	9			€ 1.048,8600
PAAS05	IndustrySt andard	PaaSDB	Oracle dbms Standard	1			€ 5.995,9400
PAAS03	IndustrySt andard	PaaSDB	SQL server	2			€ 8.629,6400
DP02	IndustrySt andard	DataProtection	Backup	19			€ 6.159,0400
DP03	IndustrySt andard	DataProtection	Golden copy	9			€ 3.500,9100
SP-07	ServiziMig razione	FiguraMigrazione	Project Manager	4		€ 1.487,2000	
SP-02	ServiziMig razione	FiguraMigrazione	Database Specialist and Administrator	20		€ 4.986,2000	
SP-12	ServiziMig razione	FiguraMigrazione	System and Network Administrator	26		€ 7.733,4400	
SP-04	ServiziMig razione	FiguraMigrazione	Cloud Application Specialist	26		€ 8.199,1000	
SP-06	ServiziMig razione	FiguraMigrazione	Enterprise Architect	6		€ 2.491,8600	
SP-23	ServiziMig razione	FiguraMigrazione	Systems Architect	5		€ 2.418,7000	
SP-07	ServiziPro fessionali	ITInfrastructureServiceOperation	Project Manager	60		€ 22.308,0000	
SP-02	ServiziPro fessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	300		€ 74.793,0000	
SP-12	ServiziPro fessionali	ITInfrastructureServiceOperation	System and Network Administrator	380		€ 113.027,2000	
SEC01	IndustrySt andard	Security	Antivirus	5			€ 2.094,0500
SP-07	ServiziPro fessionali	SecurityProfessionalServices	Project Manager	5		€ 1.859,0000	
SP-13	ServiziPro fessionali	SecurityProfessionalServices	Security Principal	10		€ 5.205,2000	
SP-14	ServiziPro fessionali	SecurityProfessionalServices	Senior Information Security Consultant	10		€ 4.237,7000	
SP-15	ServiziPro fessionali	SecurityProfessionalServices	Junior Information Security Consultant	11		€ 3.271,8400	
SP-01	ServiziPro fessionali	SecurityProfessionalServices	Cloud Application Architect	10		€ 3.873,5000	
SP-04	ServiziPro fessionali	SecurityProfessionalServices	Cloud Application Specialist	11		€ 3.468,8500	
SP-16	ServiziPro fessionali	SecurityProfessionalServices	Security Solution Architect	25		€ 10.594,2500	
SP-17	ServiziPro fessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	40		€ 17.846,4000	
SP-18	ServiziPro fessionali	SecurityProfessionalServices	Junior Security Analyst	15		€ 4.233,7500	
SP-19	ServiziPro fessionali	SecurityProfessionalServices	Senior Penetration Tester	5		€ 1.859,0000	
SP-20	ServiziPro fessionali	SecurityProfessionalServices	Junior Penetration Tester	10		€ 2.606,6000	
SP-22	ServiziPro fessionali	SecurityProfessionalServices	Data Protection Specialist	10		€ 3.718,0000	

Polo Strategico Nazionale

9 RENDICONTAZIONE

Di seguito, viene riportato un prospetto contenente la modalità di distribuzione dei servizi professionali, distinti per tipologia. I canoni dell'infrastruttura saranno attivati una volta resi disponibili i relativi servizi. La consuntivazione avverrà su base SAL mensili in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali.
Il SAL bimestrale (T0 + 2 mesi = T1) previsto a seguito del collaudo per la consuntivazione dei servizi di IT Infrastructure Service Operations (setup e collaudo) è il seguente:

Figura professionale	Quantità	Tariffa giorno/persona	Totale
Project Manager	4	371,80 €	1.487,20 €
Database Specialist and Administrator	20	249,31 €	4.986,20 €
System and Network Administrator	26	297,44 €	7.733,44 €
Cloud Application Specialist	26	315,35 €	8.199,10 €
Enterprise Architect	6	415,31 €	2.491,86 €
Systems Architect	5	483,74 €	2.418,70 €
Totale			**27.316,50 €**

Il SAL mensile previsto per la consuntivazione dei servizi di IT Service Operations è il seguente:

Figura professionale	Quantità	Tariffa giorno/persona	Totale
Project Manager	1	371,80 €	371,80 €
Database Specialist and Administrator	5	249,31 €	1.246,55 €
System and Network Administrator	6	297,44 €	1.784,64 €
Totale			**3.402,99 €**

Tale SAL sarà ripetuto ogni mese per 5 anni dalla data di collaudo, eccezion fatta per il dodicesimo mese di ogni anno (per il primo anno: T1+12 mesi), che sarà rendicontato come segue:

Figura professionale	Quantità	Tariffa giorno/persona	Totale
Project Manager	1	371,80 €	371,80 €
Database Specialist and Administrator	5	249,31 €	1.246,55 €
System and Network Administrator	10	297,44 €	2.974,40 €
Totale			**4.592,75 €**

I Security Professional Services saranno rendicontati mensilmente come di seguito riportato.

Polo Strategico Nazionale

Primo anno
SAL mensile: 1.087,09 €

Anni successivi
SAL mensile: 1.036,02 €

Di seguito un prospetto relativo alla consuntivazione dei servizi professionali per i primi 14 mesi di contratto:

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
		€ TOT														
- Setup	0%	€														
- Collaudo	100%	€ 27.317		€ 27.317												
Servizi professionali (canone mensile avanzamento/task)		€ TOT														
- IT Infrastructure Service Operation		€ 210.128			€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 3.403	€ 4.593
- Security Professional Services		€ 62.774			€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.087	€ 1.036	€ 1.036

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

22-0D-BC-48-C1-ED-80-D4-4C-F2-52-5D-49-17-27-99-63-77-F0-E3

PAdES 1 di 2 del 29/09/2023 09:32:38

Soggetto: EMANUELE IANNETTI TINIT-NNTMNL67S14H501Y

Validità certificato dal 26/10/2022 10:18:31 al 25/10/2025 10:18:31

Rilasciato da Telecom Italia Trust Technologies S.r.l. con S.N. 3AC

TimeStamp 2 di 2 del 29/09/2023 09:32:38

Soggetto: Time Stamp Server - 2

Validità certificato dal 01/01/0001 00:00:00 al 01/01/0001 00:00:00

Rilasciato da Telecom Italia Trust Technologies S.r.l. con S.N. D

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

C1-07-51-9D-E5-8F-70-DC-5F-DE-08-8E-1A-A0-11-84-62-4C-7B-03

CAdES 1 di 4 del 13/10/2023 12:31:52

Soggetto: Carlo Picco PCCCRL60E17L013P

Validità certificato dal 15/07/2022 13:20:59 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC46

CAdES 2 di 4 del 12/10/2023 15:51:51

Soggetto: Gianluca Ghiselli GHSGLC63C13L833N

Validità certificato dal 15/07/2022 13:40:29 al 15/07/2025 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT con S.N. 0174 EC90

CAdES 3 di 4 del 12/10/2023 15:48:18

Soggetto: Alessandro Mazzantini MZZLSN77A22G702G

Validità certificato dal 03/05/2023 13:54:17 al 03/05/2026 02:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT con S.N. 010D F350

CAdES 4 di 4 del 03/10/2023 15:31:49

Soggetto: SALVATORE SCARAMUZZINO SCRSVT86A01D976L

Validità certificato dal 20/09/2022 10:09:36 al 20/09/2025 10:09:36

Rilasciato da ArubaPEC EU Qualified Certificates CA G1, ArubaPEC S.p.A., IT con S.N. 77DE 32CB EE
