Polo Strategico Nazionale

Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 09/06/2025 11:33
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

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

CUP: J51B21005710007

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

AORN SANTOBONO

2025-0000006854100630-PPdF-P9R1

Questo documento contiene informazioni "confidenziali" di proprietà esclusiva della società PSN S.p.A. né il documento né sue parti possono essere pubblicate, riprodotte, copiate o comunque divulgate senza autorizzazione scritta dell'azienda oltre quanto previsto dalla lista di distribuzione

SOMMARIO

1 PREMESSA 6
2 AMBITO 7
3 DOCUMENTI 8
3.1 DOCUMENTI CONTRATTUALI 8
3.2 DOCUMENTI DI RIFERIMENTO 8
3.3 DOCUMENTI APPLICABILI 9
4 ACRONIMI 10
5 PROGETTO DI ATTUAZIONE DEL SERVIZIO 11
5.1 SERVIZI PROPOSTI 11
5.2 PUBLIC CLOUD PSN MANAGED 12
5.2.1 Descrizione del servizio 12
5.2.2 Personalizzazione del servizio 15
5.2.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi) 16
5.2.4 Specifiche di collaudo 16
5.3 CONSOLE UNICA 16
5.3.1 Overview delle caratteristiche funzionali 16
5.3.2 Modalità di accesso 18
5.3.3 Interfaccia applicativa della Console Unica 18
5.4 SERVIZI E PIANO DI MIGRAZIONE 20
5.4.1 Piano di attivazione e Gantt 22
5.5 SERVIZI PROFESSIONALI 23
5.5.1 IT infrastructure service operations 23
6 FIGURE PROFESSIONALI 25
7 SICUREZZA 26
8 CONFIGURATORE 27
9 Rendicontazione 28

Indice delle tabelle

Tabella 1: Informazioni Documento 4
Tabella 2: Autore 4
Tabella 3: Revisore 4
Tabella 4: Approvatore 4
Tabella 5 Documenti Contrattuali 8
Tabella 6: Documenti di riferimento 9
Tabella 7: Documenti Applicabili 9
Tabella 8: Acronimi 10
Tabella 9: Servizi Proposti 11

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Prima Emissione	1.1	22 Maggio 2025

Tabella 1: Informazioni Documento

Autore:	
	TIM

Tabella 2: Autore

Revisione:	
PSN Solution team	n.a.

Tabella 3: Revisore

Approvazione:	
Cloud Engineering & Migration/ Solution Design PSN Commercial team	Andrea Tomei Riccardo Rossi

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Solution
- Funzione Technology & Information
- Funzione Information Security
- Referente Servizio
- Direttore Servizio

ESTERNA A:

- Referente Contratto Esecutivo: Ing. Giuseppe D'anna
  - Email: g.danna@santobonopausilipon.it

- Referente Tecnico: Fabrizia De Martino
  - Email: f.demartino@santobonopausilipon.it

- Referente di sicurezza: Fabrizia De Martino
  - Email: f.demartino@santobonopausilipon.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'AORN SANTOBONO 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 **2025-0000006854100630-PdF-P9R1**) **opportunamente analizzate e circoscritte alle attività previste dalla Convenzione PSN**.

2 AMBITO

L'AORN Santobono-Pausilipon intende rivedere l'architettura applicativa di riferimento dei propri sistemi di Data Analytics attraverso la riprogettazione di un DB Oracle che, integrandosi con il DWH BW già in uso presso l'Azienda, consentirà la progressiva dismissione delle tabelle di frontiera in favore di web services in linea con le specifiche del protocollo HL7-FHIR. Tale attività è, inoltre, propedeutica a garantire l'alimentazione in real time e/o quotidiana (in funzione della tipologia di flusso informativo) dei propri applicativi. Si precisa che il flusso dati seguirà un andamento monodirezionale dal layer Fornitore dei sistemi sorgente verso il DB Oracle, le comunicazioni di ritorno sono da intendere nei soli casi di eventuali errori di validazione. Tale esigenza deriva dalla volontà di assicurare che le nuove soluzioni tecnologiche siano implementate e integrate in modo uniforme e tempestivo e garantiscano l'efficienza complessiva del sistema informativo in linea con le necessità istituzionali ed operative dell'AORN Santobono Pausilipon.
A tal fine, l'AORN Santobono ritiene necessario di dotarsi di Oracle Cloud Infrastructure (OCI) al fine di garantire

1. Sicurezza avanzata: Garantisce standard di sicurezza enterprise con crittografia, gestione degli accessi e conformità internazionale.
2. Prestazioni elevate: Offre affidabilità e velocità grazie a hardware di qualità come Exadata.
3. Scalabilità e flessibilità: Adatto a ogni tipo di carico, dalle applicazioni aziendali al machine learning.
4. Funzionalità autonome: Automatizza la gestione di database e infrastrutture per semplificare le operazioni.

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Documento
#1	Piano dei Fabbisogni di Servizio
#2	Piano di Sicurezza
#3	Piano di Qualità
#4	Piano di Continuità Operativa

Tabella 5 Documenti Contrattuali

Di seguito, è mostrato il link per consultare la documentazione aggiornata:

https://www.polostrategiconazionale.it/obiettivo-cloud/documentazione/

Qualificazioni Servizi Cloud disponibili al Catalogo delle Infrastrutture digitali e dei Servizi cloud-ACN:

https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

Piano della Sicurezza	Su richiesta, ed in versione ristretta. Il Sistema di Gestione della Sicurezza delle informazioni di PSN, di cui il Piano della Sicurezza è un documento, è certificato a Norma ISO 27001. Il certificato è pubblicato sul sito PSN alla sezione Documentazione.
Piano di continuità operativa	Su richiesta, ed in versione ristretta. Il Sistema di Gestione della Continuità Operativa di PSN, di cui il PCO (Piano di Continuità Operativa) è un documento, è certificato a Norma ISO 22031. Il certificato è pubblicato sul sito PSN alla sezione Documentazione

3.2 DOCUMENTI DI RIFERIMENTO

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

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

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

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

Tabella 7: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
CMP	Cloud Management Platform
CRC	Cyclic Redundancy Check
CSP	Cloud Service Provider
DB	DataBase
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
MSP-PSN	Managed Service Provider – Polo Strategico Nazionale
PA	Pubblica Amministrazione
PSN	Polo Strategico Nazionale
VM	Virtual Machine
WBT	Web Based Training
WORM	Write Once, Read Many

Tabella 8: Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

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

5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
PUBLIC CLOUD PSN MANAGED	

Tabella 9: Servizi Proposti

Le responsabilità di sicurezza fra cliente e provider sono rappresentate nelle "Matrici di Responsabilità Condivisa di Sicurezza", pubblicate sul sito di Polo Strategico Nazionale al link: https://www.polostrategiconazionale.it/chi-siamo/sicurezza/matrici-di-responsabilita-condivisa-della-sicurezza/ in aggiornamento alla Matrice presente in Convezione (Figura 16, pag.100 del Progetto di Fattibilità).

I dati trattati sono di tipo critico come da classificazione ACN.

5.2 PUBLIC CLOUD PSN MANAGED

5.2.1 Descrizione del servizio

Il Public Cloud PSN Managed è un servizio PSN Core che permette alle PA di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica degli ambienti e gestione operata da personale PSN.

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

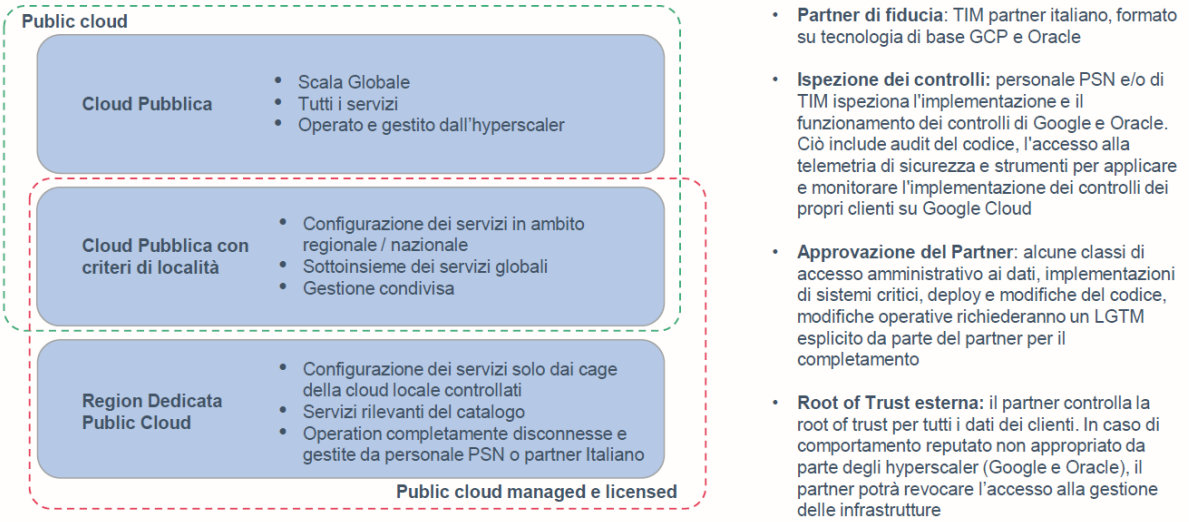


Figura 1 Public Cloud vs Public Cloud Managed

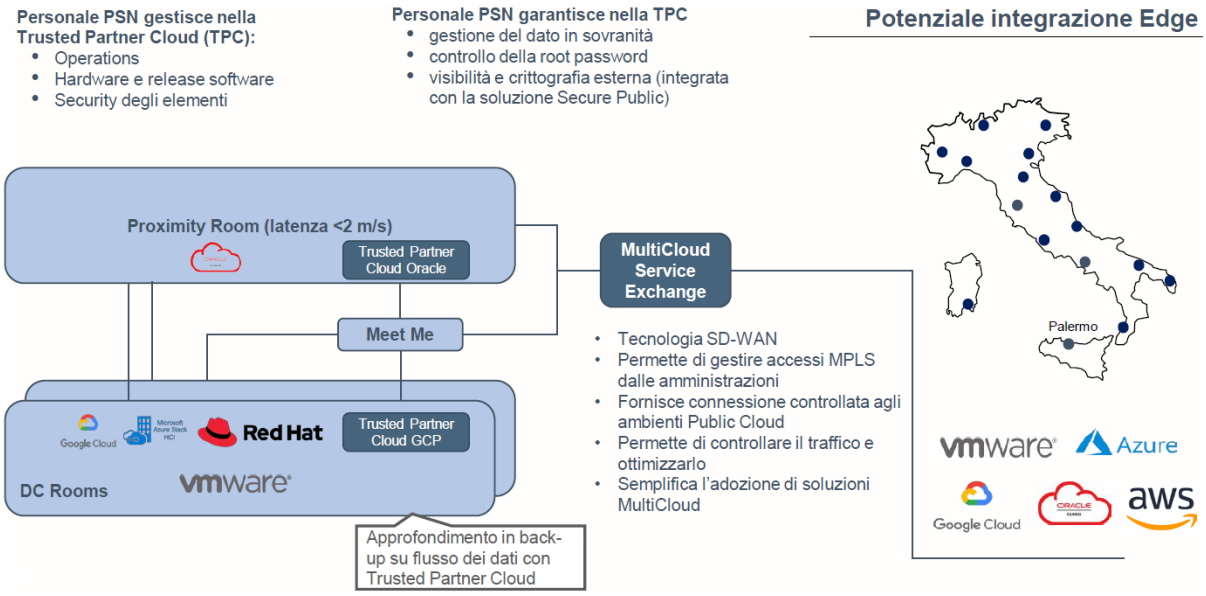


Figura 2 Architettura Public Cloud Managed

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

GCP (Google Cloud Platform)

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

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

Oracle Cloud

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

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

Il servizio

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

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

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

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

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

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

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

Rientra inoltre sotto il controllo dell'MSP-PSN anche tutta la gestione delle key chains: nomi di dominio, certificati TLS, CA, rotazione delle chiavi, scadenza, ecc.

Encryption at-rest

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

Gestione degli Aggiornamenti

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

Modello di Supporto

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

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

5.2.2 Personalizzazione del servizio

Le risorse utili alla migrazione sono riportate nella tabella di seguito:

Infrastruttura OCI			
Servizio	**Unit**	**Q.tà YR**	**Q.tà TOT**
OCI - API Gateway - 1,000,000 API Calls	1,000,000 API Calls Per Month	1	12
OCI - External Key Management	Key Version Per Month	1	12
OCI - FastConnect 1 Gbps	Port Hour	2	17520
OCI - Monitoring - Ingestion	Million Datapoints	100	100
OCI - Monitoring - Retrieval	Million Datapoints	100	100
OCI - Oracle Integration Cloud Service - Enterprise	5K Messages Per Hour	2	17520
OCI - Streaming - PUT or GET	Gigabytes of Data Transferred	100	100
OCI - Streaming - Storage	Gigabyte Per Hour	10	87600

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, qualora non lo siano, entro un ragionevole lasso temporale. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN

provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17).

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

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

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

5.2.4 Specifiche di collaudo

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

5.3 CONSOLE UNICA

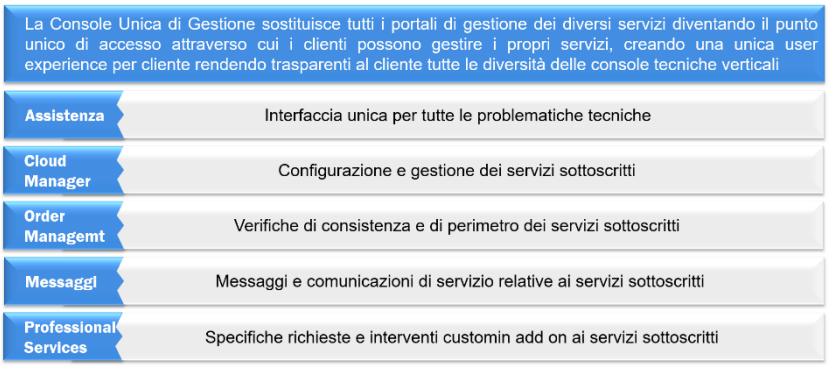
La Fornitura prevede l'erogazione alle PAC, in maniera continuativa e sistematica, di una serie di servizi afferenti ad un Catalogo predefinito e gestito attraverso una Console Unica dedicata.
Il PSN metterà a disposizione delle Amministrazioni Contraenti una piattaforma di gestione degli ambienti cloud 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

Figura 3 Funzionalità CU

e abilita i sottoscrittori ad accedere in maniera semplificata agli strumenti che consentono di: √gestire in modalità integrata i profili di accesso alla CU tramite le funzionalità di Identity Management; disegnare l'architettura dei servizi acquistati e gestirne le eventuali variazioni; √consentire l'interfacciamento attraverso le API per la gestione delle risorse istanziate ma anche per definire un modello di IaC (Infrastructure as Code); segnalare eventuali anomalie in modalità "self".



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

1. Area Attivazione contrattuale. All'atto dell'adesione alla convenzione da parte dell'Amministrazione, sulla CU: √saranno caricati i dati contrattuali ed anagrafici dell'Amministrazione; √generato il profilo del referente Master (Admin) della PA a cui sarà inviata una "Welcome Letter" con il link della piattaforma, l'utenza e la password (da modificare al primo login) per l'accesso alla CU; √sarà configurato il tenant dedicato alla PA, che rappresenta l'ambiente cloud tramite il quale la PA usufruirà dei servizi acquisiti (IaaS, PaaS, ecc.).
2. Area Access Management e profilazione utenze. L'accesso alla CU è gestito totalmente dal sistema di Identity Access Management (IAM). Gli utenti, previa registrazione, saranno censiti nello IAM, e con le credenziali rilasciate potranno accedere dalla console alle risorse allocate all'interno del proprio tenant. Anche la creazione dei profili delle utenze e la loro associazione con gli account degli utenti sarà gestita tramite le funzionalità di IAM in un'apposita sezione della CU denominata "Gestione Utenze".
3. Area Design & Delivery. Attraverso tale modulo della CU, l'Amministrazione Contraente potrà configurare in autonomia i servizi acquistati secondo le metriche definite per la convenzione, costruendo, anche mediante l'utilizzo di un tool di visualizzazione, la propria architettura cloud sulla base delle risorse contrattualizzate. Successivamente la CU, interagendo in tempo reale attraverso le API dei servizi cloud verticali, consentirà l'immediata attivazione delle risorse e dei servizi previsti nell'architettura attraverso la creazione di uno o più tenant logici per segregare le risorse computazionali dei clienti (Project). Il processo è gestito mediante un workflow automatizzato di delivery implementato tramite l'uso di Blueprint. La CU esporrà anche delle API affinché la singola Amministrazione Contraente possa interagire attraverso i propri tools di CD/CI, IaC (Terraform, Ansible...) oppure attraverso una propria CU come ulteriore livello di astrazione e indipendenza (qualora ne avesse già a disposizione e quindi creare una CU Master Controller che interagisce con quella del PSN appunto via API).
4. Area Management & Monitoring. La piattaforma consentirà ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali. Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e

bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.

5. Area Self Ticketing. Consente alla PA di segnalare in modalità self le anomalie riscontrate sui servizi cloud contrattualizzati.

5.3.2 Modalità di accesso

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

5.3.3 Interfaccia applicativa della Console Unica

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

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

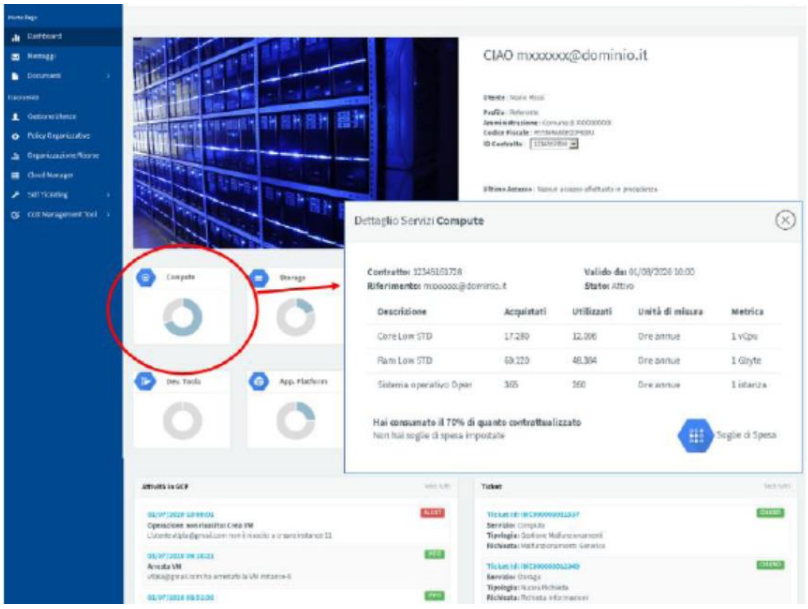


Figura 4 Dashboard CU

- Cloud Manager: in questa sezione, per tutti i servizi della convenzione, ciascuna Amministrazione potrà, nell'ambito della funzione di Design & Delivery:

- costruire l'architettura cloud di ciascun Project all'interno del proprio tenant;
- attivare i servizi in self-provisioning;
- nell'ambito della funzione di Management & Monitoring:
- effettuare operazioni di scale up e scale down sui servizi contrattualizzati;
- gestire e monitorare tali servizi accedendo direttamente all'opportuna sezione della console.

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

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

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

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

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

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

5.4 SERVIZI E PIANO DI MIGRAZIONE

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

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

Si chiede alla PA la disponibilità di fornire uno o più referenti coi quali il Project Manager Contratto di Adesione e il Technical Team Leader del PSN si possano interfacciare.
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 5: Servizio di Migrazione - Metodologia EMG2C

<NOTA: i segg. paragrafi dettagliano il processo di migrazione standard sopra descritto. Possono essere adottati a seconda dell'applicabilità al Piano di Migrazione per la specifica PA per migliorare la qualità espositiva del documento:

1. **Analisi e Discovery**

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

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

In particolare questa fase di occuperà di reperire le informazioni:

a) delle piattaforme oggetto della migrazione;
b) delle applicazioni erogate dalla PA
c) dei dati oggetto di migrazione;
d) degli SLA delle singole applicazioni;
e) di eventuali finestre utili per la migrazione;
f) di eventuali periodi di indisponibilità delle applicazioni;
g) del Cloud Maturity Model;
h) analisi della sicurezza delle applicazioni e dell'ambiente da migrare;
i) Energy Optimization.

Inoltre, la Discovery ha lo scopo di raccogliere tutte le informazioni relative all' infrastruttura e ai workload da migrare. Questa attività consente di comporre un inventory ed una check list che supporteranno le successive attività e permetteranno, in fase di collaudo, la verifica di tutte le componenti migrate.
In funzione dei risultati dell'Assessment, si valuterà la **strategia ottimale di migrazione** verso l'ambiente target, in funzione dei seguenti driver:

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

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

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

2. **Set-up**

Rappresenta la fase propedeutica all'effettiva esecuzione della migrazione ed è finalizzata a garantire un'efficace predisposizione dell'ambiente target su cui dovranno essere movimentati i servizi/applicazioni dell'Amministrazione e si articola nelle seguenti fasi:

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

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

3. **Migrazione**

Tale fase si articola nei seguenti step:

- Trasferimento dei workload e conseguente esecuzione di test "a vuoto" dell'ambiente migrato;
- Trasferimento dei dati, ovvero esecuzione dell'effettivo spostamento dei dati dal Data Center dell'Amministrazione all'interno dell'infrastruttura del PSN;
- Implementazione delle Policy di Sicurezza;
- Impostazione del monitoraggio.

4. **Collaudo**

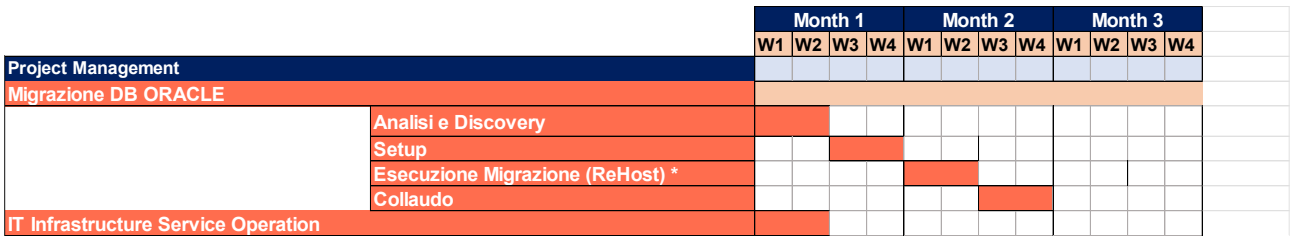
Definizione Strategia di Collaudo: tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo delle applicazioni migrate nell'ambiente target.

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

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

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.



5.5 SERVIZI PROFESSIONALI

Sono resi disponibili all'Amministrazione servizi di evoluzione con l'obiettivo di: ✓migliorare eventuali ambienti precedentemente migrati sulla piattaforma PSN tramite Re-Host o tramite i servizi di Housing/Hosting; ✓ supportare la migrazione di applicativi on premise verso una piattaforma cloud tecnologicamente avanzata, in modo da beneficiare delle funzionalità messe a disposizione dall'infrastruttura proposta, come sicurezza, scalabilità e ottimizzazione di costi e risorse.
In particolare, i due servizi proposti sono quelli di Re-Platform e Re-Architect, in quanto queste due strategie di migrazione sono quelle che maggiormente massimizzano i benefici per l'Amministrazione di una piattaforma cloud come quella oggetto del presente progetto.
I due servizi si differenziano principalmente per la quantità del codice applicativo che viene modificato e, di conseguenza, per le tempistiche di attuazione. Il Re-platform modifica solamente alcuni componenti senza impattare il core dell'applicativo, mentre il Re-architect permette di portare l'applicazione in Cloud attraverso interventi puntuali sulla stessa.
Tali servizi non sono necessariamente alternativi ma possono eventualmente rappresentare fasi sequenziali di un programma di modernizzazione **applicativa**.
Per questi servizi, in base alla specifica esigenza, viene proposto un **team mix** composto dai profili professionali elencati in precedenza.

5.5.1 IT infrastructure service operations

In seguito all'avvenuta migrazione, il PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni. 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.

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:

- **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.

7 SICUREZZA

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

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

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

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

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

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

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

8 CONFIGURATORE

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

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	6854100630
Ragione Sociale	AORN SANTOBONO
IDENTIFICATIVO DOCUMENTO	
Emesso da	PSN Commercial/CTIO
Codice Documento	2025-0000006854100630-PPdF-P9R1
Versione	1

VERSIONE CONFIGURATORE	7.2.2

RIEPILOGO PREZZI

SERVIZIO	Totale UT	Totale Canone Annuale
Industry Standard	€ -	€ -
Hybrid Cloud on PSN Site		€ -
SecurePublicCloud		€ -
Public Cloud PSN Managed		€ 31.825,96
Servizi di Migrazione	€ -	
Servizi Professionali	€ 3.088,60	
TOTALE	€ 3.088,60	€ 31.825,96

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
	SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	10		€ 3.088,60	
		PublicCloudPSNManaged	Compute - Compute Engine					7.917,02 €
		PublicCloudPSNManaged	Identity & Security - Cloud Operations					€ 7.536,05
		PublicCloudPSNManaged	Networking - Partner Interconnect					€ 4.386,67
		PublicCloudPSNManaged	Storage - Storage					€ 11.986,22

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

Servizio	UT	Canone Annuo
Public Cloud PSN Managed		€ 31.825,96
Servizi Professionali	€ 3.088,60	
TOTALE	**€ 3.088,60**	**€ 31.825,96**

Si prevede di effettuare i seguenti Stati di Avanzamento Lavori (SAL).

- ✓ **N° 1 SAL da prevedere nell'intervallo di tempo massimo [T_0 : T_1=(T_0 + 1 mese)]:**

Servizio	Figura Professionale	Quantità	Importo
Servizi Professionali	System and Network Administrator	10	€ 3.088,60
Totale (Iva Esclusa)			**€ 3.088,60**