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

PROVINCIA DI PADOVA

SOMMARIO

Indice delle tabelle

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Primo rilascio	1	25/01/2024

Tabella 1: Informazioni Documento

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

Tabella 2: Autore

Revisione:	
PSN Solution team	n.a.

Tabella 3: Revisore

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

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

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

ESTERNA A:

- Referente Contratto Esecutivo PROVINCIA DI PADOVA Luca DAINESE
  - Email: luca.dainese@provincia.padova.it
- Referente Tecnico PROVINCIA DI PADOVA Marco PENNA
  - Email: marco.penna@provincia.padova.it

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del **PSN** relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012.
Quanto descritto, è stato redatto in conformità alle richieste del ***PROVINCIA DI PADOVA*** 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 **2023-0000080006510285-PdF-P1R1**).

2 AMBITO

2.1 Obiettivi

Gli obiettivi per cui l'amministrazione richiede di aderire ai servizi del PSN sono la messa in sicurezza dell'attuale infrastruttura informatica on-premise dell'ente prevedendo la migrazione di alcuni servizi informatici di base, i portali web istituzionali, le applicazioni di front office e back office con codice sorgente di proprietà dell'Amministrazione, al servizio sia degli uffici interni che di Enti terzi convenzionati (per lo più Comuni del territorio provinciale).

Servizio dell'amministrazione	Tipo di Migrazione
Servizi ICT di base (autenticazione utenti, sistemi di sicurezza e gestione base dati)	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Servizi Web di back-office per utenti interni ed esterni (Intranet/Extranet Aziendale, Intranet del CST e applicazioni web)	Modalità A - trasferimento in sicurezza dell'infrastruttura IT
Servizi di comunicazione istituzionale e servizi digitali per i cittadini e le imprese (Portali e Servizi Web)	Modalità A - trasferimento in sicurezza dell'infrastruttura IT

Tabella 5: servizi dell'amministrazione

2.1.1 Servizi ICT di base

I servizi denominati "Servizi ICT di base" fanno riferimento a tutte le categorie di software che verranno implementati nel PSN, il cui compito sarà quello di fornire servizi di base "back-end" ad altri servizi denominati di front-end. I servizi, che saranno necessariamente i primi ad essere implementati tramite l'installazione di alcune VM, prevedono le seguenti funzionalità:

Autenticare in modo sicuro gli utenti:

Il servizio sarà implementato tramite l'installazione di n.2 VM con sistema operativo rispettivamente Microsoft Windows e Linux nelle quali verranno attivate le seguenti funzionalità:

- Active Directory – servizio per la gestione dell'autenticazione degli utenti;
- DNS – servizio per la risoluzione dei nomi di rete;
- DHCP – servizio per l'assegnazione automatica e centralizzata degli indirizzi IP;
- Radius – servizio per gestire l'autenticazione degli utenti, la configurazione e l'accounting;
- OpenLDAP – servizio per la gestione dell'autenticazione di alcune tipologie di utenti non gestibili tramite Active Directory;

Aumentare la sicurezza dei servizi esposti verso la rete Internet:

Il servizio prevede l'installazione di un sistema di "reverse proxy" che permette di operare come un port forwarding, inoltrando verso i server della rete interna le richieste che provengono dall'esterno in base all'intestazione della chiamata. Inoltre, permetterà:

- Oscuramento ai client delle caratteristiche di uno o più server collocati nella rete locale;
- Riscrittura del URL;

- Cifratura HTTPS;
- Accesso a più server sfruttando un solo IP.

Questo servizio verrà posto a monte degli altri servizi basati di tipo Web che verranno esposti in Internet e dei futuri servizi che verranno migrati nel PSN.

Gestire la sicurezza perimetrale e le reti private virtuali (VPN):

Il servizio verrà implementato utilizzando tecnologie di firewalling di ultima generazione e avrà il compito di proteggere tutti gli altri servizi accessibili da Internet e permettere tramite "tunnel VPN" la comunicazione sicura tra i servizi migrati nel PSN e i restanti servizi presenti on-premise.

Gestire gli archivi dei dati:

Il servizio prevede l'implementazione della gestione di tutti i vari archivi informatici dei vari servizi rivolti sia all'utenza interna che esterna tramite l'uso del motore di database relazionale Oracle previsto dal servizio gestito del PSN come PaaS.

2.1.2 Servizi Web di back-office per utenti interni ed esterni

I servizi Web di back-office per utenti interni ed esterni sono:

Intranet:

Il servizio è utilizzato sia all'interno che all'esterno dell'ente ed è composto da una serie di moduli software ciascuno con una propria autonomia e funzionalità. Di seguito elenchiamo i moduli più importanti:

- Helpdesk: modulo per la gestione dei ticket per il supporto tecnico agli utenti da parte dei tecnici del servizio sistemi informativi dell'ente
- Rubrica;
- Inventario dell'hardware e del software utilizzato dall'ente;
- Gestione invio massivo di messaggi SMS per avvisi esterni;
- Documentazioni generica sull'organizzazione dell'ente (es. news, comunicazioni al personale, ecc.);
- Gestione del SSON verso applicativi terzi;
- Gestione delle prenotazioni appuntamenti per pratiche di cittadini stranieri presso Questura e Prefettura di Padova
- Visualizzazione delle pratiche di autorizzazione ambientale per l'ARPAV

Servizio di storage:

Il servizio prevede delle quote di storage a servizio di Enti convenzionati con la Provincia tramite i servizi erogati dal CST.

Applicazioni Web:

Il servizio è utilizzato sia all'interno che all'esterno dell'ente ed è composto da una serie di moduli software ciascuno con una propria autonomia e funzionalità. Di seguito elenchiamo i moduli più importanti:

- Gestione concessioni patrimonio integrato con MyPay di Regione Veneto;
- MyPayDovuti - emissione dovuti PagoPa integrato con MyPay di Regione Veneto;
- ParixPDVam - Integrazione con servizi Parix di Regione Veneto piattaforma VAM;
- PDND - Integrazione con piattaforma nazionale servizi digitali (PDND) attualmente solo con servizio INAD (verifica domicili digitali);
- SiaWeb - Sistema informativo Ambientale Provincia di Padova di gestione delle pratiche di autorizzazione;
- Connettore con software protocollo dell'ente per erogare servizi ad applicativi verticali interni;

La migrazione di tutti i servizi sopra elencati verrà effettuata a seguito dell'implementazione dei "Servizi ICT di Base", punto 2.1.1.

2.1.3 Servizi di comunicazione istituzionale e servizi digitali per i cittadini e le imprese

Il servizio prevede l'hosting di siti web esposti in internet tra cui il portale ufficiale dell'ente.Per alcuni siti è richiesto l'accesso al servizio di database Oracle di cui al punto 2.1.1.
Nella fase di migrazione verranno effettuati degli aggiornamenti a livello applicativo con le ultime release software disponibili.

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 6: 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 7: 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 8: 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
CST	Centro Servizi Territoriali della Provincia di Padova
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
HA	High Availability
IaaS	Infrastructure as a Service
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
VM	Virtual Machine
WORM	Write Once, Read Many

Tabella 9: 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.

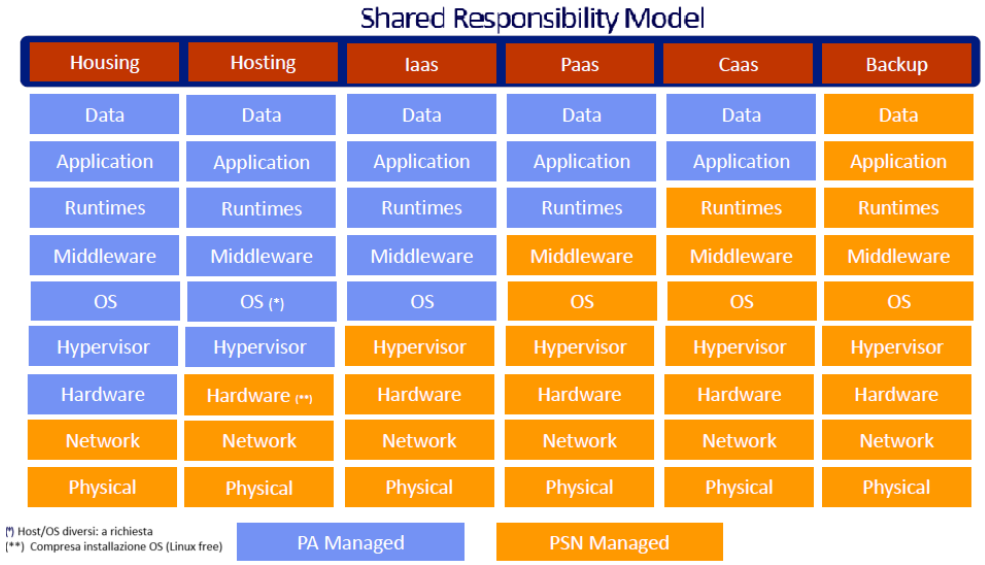
5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
Industry Standard	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	IT Infrastructure Service Operation

Tabella 10: 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 Infrastructure as a Service

5.2.1.1 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.

5.2.1.2 Personalizzazione del servizio

Negli incontri propedeutici al rilascio del piano dei fabbisogni l'amministrazione ha esplicitamente dimensionato con la nostra consulenza quanto espresso nel paragrafo 7 del piano dei fabbisogni.

Sintetizziamo qui la richiesta, congruente con quanto si evince nel paragrafo "8 Configuratore".

- 16 vCPU
- 64 GB RAM,
- 1000 GB di IaaSStorageHA - Storage High Perfomance
- 21000 GB di IaaSStorageHA - Storage Standard Perfomance
- 2 Pool di indirizzi pubblici /29
- 4 Licenze Windows Server STD CORE (2 core)

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 Platform as a Service

5.2.2.1 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:

- 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.

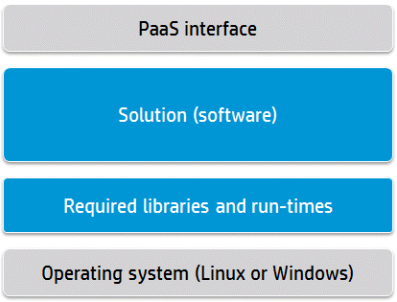


Figura 2 Platform as a Service

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.

5.2.2.2 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).

5.2.2.3 Personalizzazione del servizio

Negli incontri propedeutici al rilascio del piano dei fabbisogni l'amministrazione ha esplicitamente dimensionato con la nostra consulenza quanto espresso nel paragrafo 7 del piano dei fabbisogni.

Sintetizziamo qui la richiesta, congruente con quanto si evince nel paragrafo "8 Configuratore".

1 PaaSDB Oracle dbms Standard

- 2 vCPU
- 32 GB RAM (le 12 standard più 20 GB RAM IaaSSharedHA aggiuntivi)
- 20 GB Storage che il cliente complimenterà autonomamente con
  - 1000 GB di IaaSStorageHA - Storage HP Encrypted
- 1 indirizzo IP pubblico singolo

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

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

5.2.2.5 Specifiche di collaudo

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

5.2.3 Data Protection e Disaster Recovery

5.2.3.1 Data Protection: Backup

Servizio «self-managed» l'utente ha completa autonomia di gestione nella definizione della policy di backup. Naturalmente 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.

5.2.3.2 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.

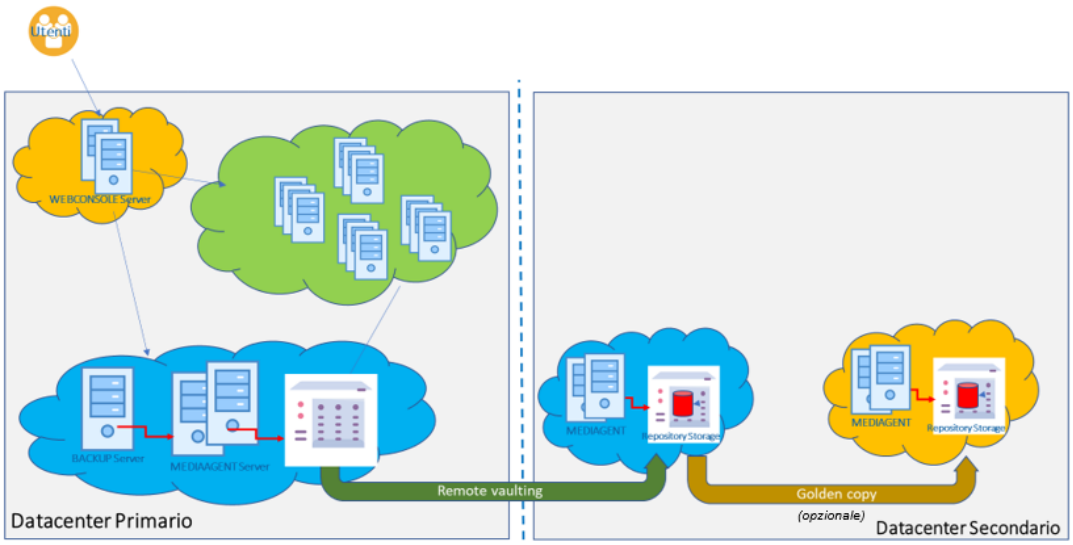


Figura 3 Architettura Funzionale Golden Copy

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.**

5.2.3.3 Personalizzazione del servizio

Abbiamo condotto col cliente una simulazione basata sul Configuratore BaaS del 23/11/2023

(1 full, 7 incrementali, variazione 10% su 1 TB di Storage HP + 1 TB di Storage HP Encrypted) ed abbiamo ottenuto uno spazio da dedicare al **backup** di IaaS e PaaSDB pari a **4TB**

Il cliente utilizzerà la **Golden Copy** per il 40% di questo storage ed avrà a disposizione **2 TB** di Golden Copy

Lo Storage Standard Performance non sarà sottoposto a backup

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.

5.3 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.

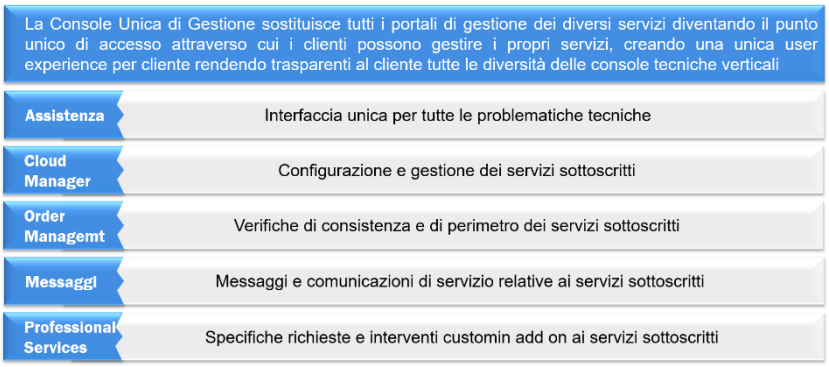
5.3.1 Overview delle caratteristiche funzionali

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

Figura 4 Funzionalità CU

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

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

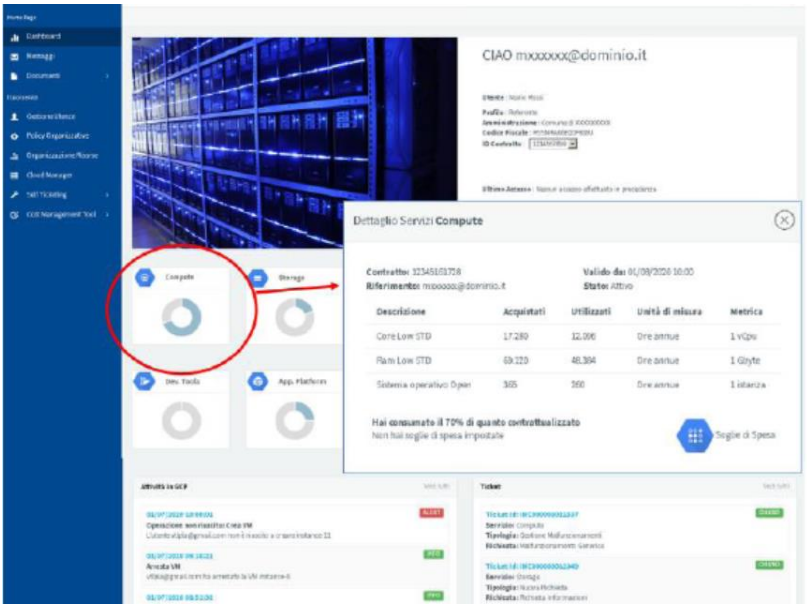


Figura 5 Dashboard CU

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.).

- 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

<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 migrazione

Si riporta di seguito iI piano di migrazione che fornisce un quadro sintetico del progetto di migrazione dell'Amministrazione

Nome servizio	Classificazione dei Dati	Tipo di migrazione	Budget – Costi di migrazione	Budget - Canone annuale	Previsione tempi Migrazione
Servizi ICT di base (autenticazione utenti, sistemi di sicurezza e gestione base dati)	Ordinari	modalità B	25.000 €	8.000 €	3 mesi
Servizi Web di back-office per utenti interni ed esterni (Intranet/Extranet Aziendale, Intranet del CST e applicazioni web)	Ordinari	modalità A	20.000 €	8.000 €	6 mesi
Servizi di comunicazione istituzionale e servizi digitali per i cittadini e le imprese (Portali e Servizi Web)	Ordinari	modalità A	20.000 €	7.000 €	6 mesi

Tabella 11: vincoli di migrazione dei servizi

5.4.2 Tempistiche

Nome servizio	T1 Analisi & Discovery	T2 Setup	T3 Migrazione	T4 Collaudo
Servizi ICT di base	T0 + 10 giorni	T1 + 10 giorni	T2 + 2 mesi	T3 + 10 giorni
Servizi Web di back-office per utenti interni ed esterni	T0 + 10 giorni	T1 + 20 giorni	T2 + 1 mese	T3 + 1 mese
Servizi di comunicazione istituzionale e servizi digitali per i cittadini e le imprese	T0 + 10 giorni	T1 + 20 giorni	T2 + 1 mese	T3 + 1 mese

Tabella 12: tempistiche migrazione

5.4.3 Piano di attivazione e Gantt

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

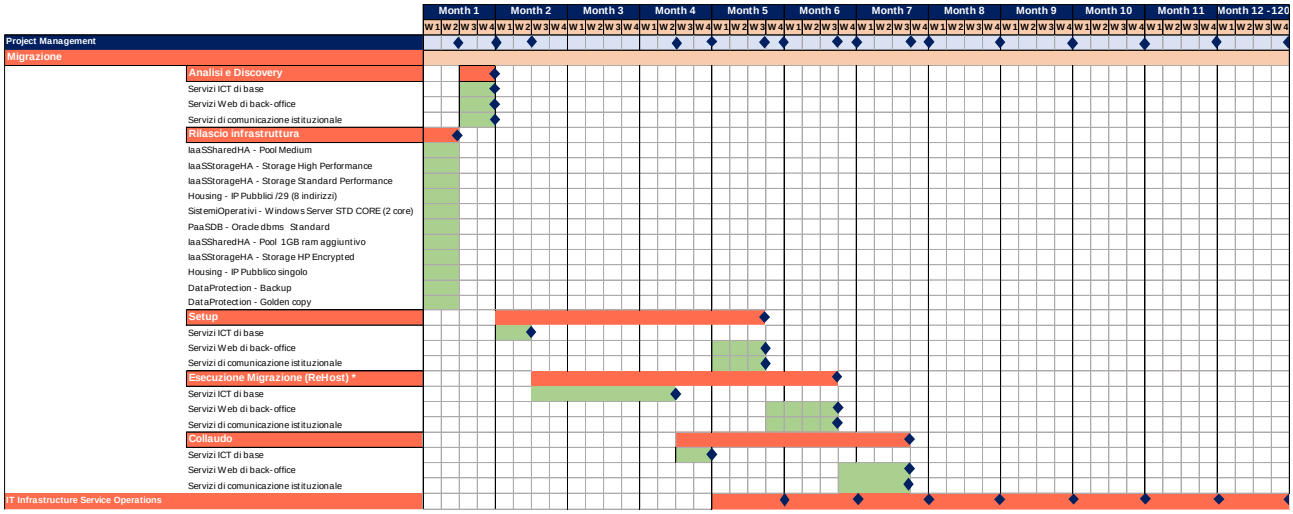


Figura 7: GANTT

5.4.4 IT infrastructure service operations

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

- Monitoraggio
- Workload management
- Infrastructure optimization

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

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

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

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

5.4.4.1 Personalizzazione del servizio

Le figure offerte dal PSN Cloud Enabler in questo ambito servono a garantire il supporto dei servizi creati in PSN per l'intera durata del contratto.

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 Integration & Test Specialist**: Contribuisce in differenti aree dello sviluppo del sistema, effettuando il testing delle funzionalità del sistema, identificando le anomalie e diagnosticandone le possibili cause. Utilizza e promuove strumenti automatici.

7 SICUREZZA

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

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

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

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

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

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

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

8 CONFIGURATORE

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

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	00000800006510285
Ragione Sociale	PROVINCIA DI PADOVA
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-00000800006510285-PdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	4.1.1

RIEPILOGO PREZZI				
SERVIZIO	Totale UT		Totale Canone Annuale	
Industry Standard			€	22.185,91
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	-
Public Cloud PSN Managed			€	-
Servizi di Migrazione	€	57.391,39		
Servizi Professionali	€	109.395,80		
TOTALE	€	166.787,19	€	22.185,91

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
VDC_a	IAAS15	IndustrySt andard	IaaSSharedHA	Pool Medium	1			€ 2.744,4300
VDC_a	IAAS03	IndustrySt andard	IaaSStorageHA	Storage High Performance	2			€ 728,1000
VDC_a	IAAS04	IndustrySt andard	IaaSStorageHA	Storage Standard Performance	42			€ 8.378,1600
VDC_a	HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	2			€ 130,9000
	SO01	IndustrySt andard	SistemiOperativi	Windows Server STD CORE (2 core)	4			€ 466,1600
VDC_b	PAAS05	IndustrySt andard	PaaSDB	Oracle dbms Standard	1			€ 5.995,9400
VDC_b	IAAS18	IndustrySt andard	IaaSSharedHA	Pool 1GB ram aggiuntivo	20			€ 646,4000
VDC_b	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	2			€ 997,4000
VDC_b	HOUSING04	IndustrySt andard	Housing	IP Pubblico singolo	1			€ 23,8000
VDC_a	DP02	IndustrySt andard	DataProtection	Backup	4			€ 1.296,6400
VDC_a	DP03	IndustrySt andard	DataProtection	Golden copy	2			€ 777,9800
	SP-07	ServiziMigr azione	FiguraMigrazione	Project Manager	2		€ 743,6000	
	SP-03	ServiziMigr azione	FiguraMigrazione	System Integrator & Testing Specialist	7		€ 1.470,2800	
	SP-12	ServiziMigr azione	FiguraMigrazione	System and Network Administrator	44		€ 13.087,3600	
	SP-04	ServiziMigr azione	FiguraMigrazione	Cloud Application Specialist	72		€ 22.705,2000	
	SP-06	ServiziMigr azione	FiguraMigrazione	Enterprise Architect	30		€ 12.459,3000	
	SP-07	ServiziProf essionali	ITInfrastructureServiceOperation	Project Manager	30		€ 11.154,0000	
	SP-02	ServiziProf essionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	60		€ 14.958,6000	
	SP-12	ServiziProf essionali	ITInfrastructureServiceOperation	System and Network Administrator	280		€ 83.283,2000	
	SP-07	ServiziMigr azione	FiguraMigrazione	Project Manager	3		€ 1.115,4000	
	SP-01	ServiziMigr azione	FiguraMigrazione	Cloud Application Architect	15		€ 5.810,2500	

Figura 8: export del configuratore

9 Rendicontazione

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

			Milestone di avanzamento % - Gate approvativi									
Servizi di Migrazione (Milestone Based)	Peso	Importo	Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mesi dispari 9-119	Mesi pari 10-120
		€ 57.391,39										
- Analisi & Discovery	30%	€ 17.217,42	€ 17.217,42									
- Setup	30%	€ 17.217,42		€ 5.739,14			€ 11.478,28					
- Migrazione(*)	30%	€ 17.217,42						€ 17.217,42				
- Collaudo(*)	10%	€ 5.739,14							€ 5.739,14			
Servizi professionali (canone mensile avanzamento/task)		€ 109.395,80										
- IT Service Operation(**)	100%	€ 109.395,80						€ 1.823,45		€ 5.469,79		€ 1.823,26

Figura 9: rendicontazione dei servizi professionali