Polo Strategico Nazionale

IL CLOUD SOVRANO PER L'ITALIA DIGITALE

Favoriamo l'innovazione e la trasformazione digitale italiana attraverso la gestione sicura dei dati e dei servizi della Pubblica Amministrazione



Agenda

1. INTRODUZIONE
2. CONTESTO DI RIFERIMENTO
3. POLO STRATEGICO NAZIONALE: PERCORSO, VANTAGGI E TECNOLOGIE
4. SOLUZIONI OFFERTE DA POLO STRATEGICO NAZIONALE
5. COME ADERIRE



Agenda

1 INTRODUZIONE

- Chi siamo
- Unique Selling Proposition

2 CONTESTO DI RIFERIMENTO

3 POLO STRATEGICO NAZIONALE: PERCORSO, VANTAGGI E TECNOLOGIE

4 SOLUZIONI OFFERTE DA POLO STRATEGICO NAZIONALE

5 COME ADERIRE



Unique Selling Proposition

Unico operatore **multicloud** al servizio della PA per la **messa in sicurezza** di dati e servizi del Paese, che accompagna la trasformazione digitale dell'Italia verso il **Journey-in-the-Cloud**

MULTICLOUD

PSN offre la possibilità di scelta tra un **cloud di proprietà PSN** oltre a **quattro Cloud Service Providers**

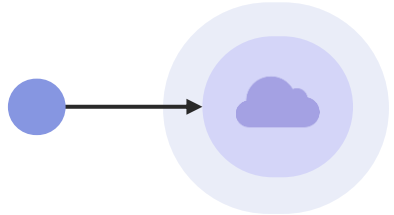


SERVIZI SECURIZZATI

Sia il Private Cloud PSN, sia i CSP pubblici, garantiscono **alti standard di sicurezza** informatica e protezione dei dati e servizi

JOURNEY-IN-THE-CLOUD

Oltre a **favorire la migrazione** verso il cloud, accompagna la PA per **10 anni** in un processo di adeguamento in ottica cloud-first, con il fine di abilitare la **trasformazione digitale del Paese**



Fonti: Razionalizzazione del Patrimonio ICT|Agenzia per l'Italia digitale (agid.gov.it)

Polo Strategico Nazionale

Agenda

1 INTRODUZIONE

2 CONTESTO DI RIFERIMENTO

- Le sfide del contesto digitale per la PA Italiana
- Strategia Cloud Italia: la risposta ai bisogni delle PA
- La classificazione di dati e servizi

3 POLO STRATEGICO NAZIONALE: PERCORSO, VANTAGGI E TECNOLOGIE

4 SOLUZIONI OFFERTE DA POLO STRATEGICO NAZIONALE

5 COME ADERIRE



Le sfide del contesto digitale per la PA Italiana

Polo Strategico Nazionale nasce dalla necessità di garantire una struttura a più alta affidabilità, resilienza e indipendenza alle amministrazioni italiane

AFFIDABILITÀ DELLE STRUTTURE

- **11.000** Data Center utilizzati dalla Pubblica Amministrazione Italiana
- Su **1.252** Data Center delle PA analizzati1 da AgID il **95%** è risultato carente in termini di sicurezza, affidabilità ed efficienza

SICUREZZA INFORMATICA

- Le **minacce informatiche** sono molteplici e sempre più frequenti
- le Pubbliche Amministrazioni sono tra i principali bersagli di **attacchi cyber**[2] a discapito dei cittadini e dei loro dati.

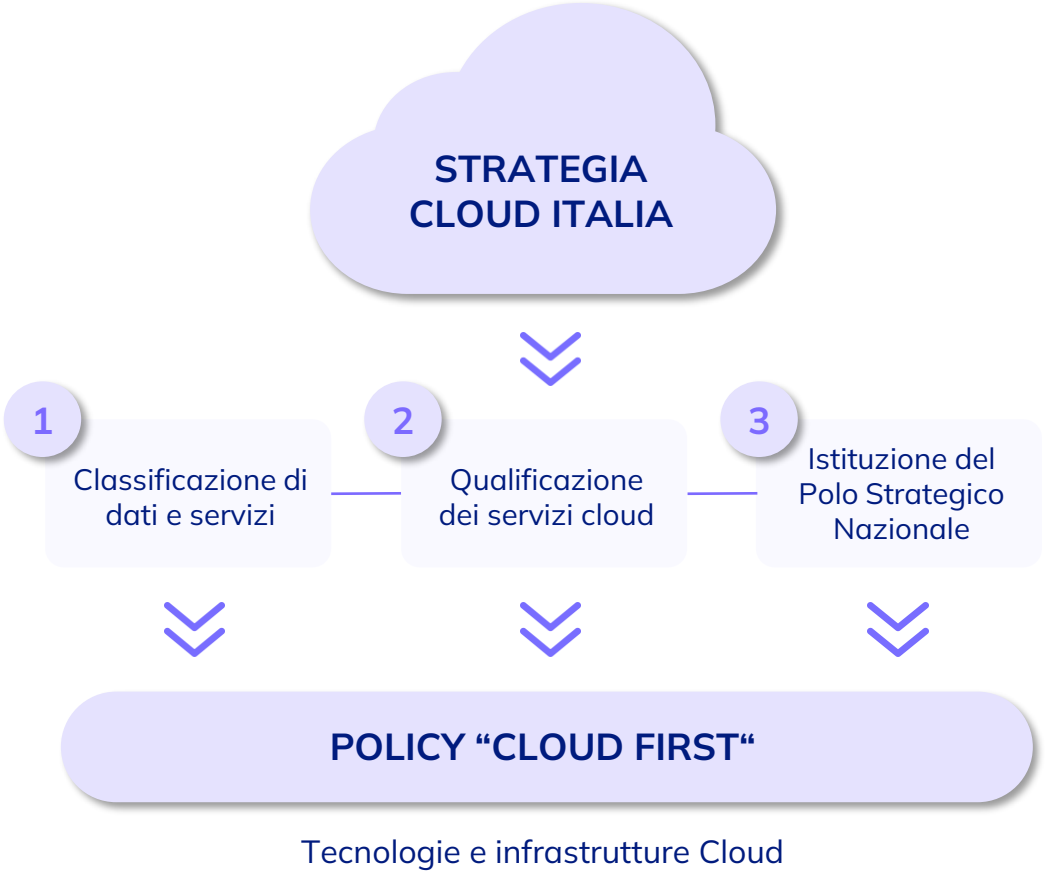
AUTONOMIA TECONOLOGICA

- Desiderio della comunità europea di avere un'**indipendenza** rispetto a società non UE che offrono servizi in ambito IT che coinvolgono dati e infrastrutture strategiche. PSN rappresenta la prima soluzione concreta per raggiungere una piena **sovranità digitale dei dati.**

[1]*Fonte: AgID Piano Italia Digitale 2026 e Censimento del Patrimonio IC*
[2]*Fonte: Relazione Annuale ACN al Parlamento 2021*

Strategia Cloud Italia: la risposta ai bisogni delle PA

Per rispondere a queste necessità delle PA, il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri e l'Agenzia per la Cybersicurezza nazionale, hanno creato la **Strategia Cloud Italia**



Obiettivi

- Assicurare **autonomia tecnologica del Paese**
- Garantire il **controllo sui dati**
- Aumentare la **resilienza** dei servizi digitali

Direttrici

- classificare i dati e i servizi attuali della PA
- qualificare i fornitori di Cloud Pubblico e i Servizi Cloud
- realizzare un'infrastruttura nazionale per erogare i Servizi di Polo Strategico Nazionale

Si basa sul principio "Cloud First", che considera prioritario per le Pubbliche Amministrazioni il ricorso a strumenti e tecnologie di tipo cloud, che garantisco la sicurezza e l'autonomia necessarie, valorizzando la PA.

Classificazione di dati e servizi

La Strategia Cloud Italia ha identificato, su indicazioni dell'Agenzia per la Cybersicurezza Nazionale, 3 tipologie di dati e servizi alla base delle strategie di migrazione al cloud delle Pubbliche Amministrazioni.

La **classificazione** dei dati e dei servizi ha lo scopo di suddividere i dati, in base alle conseguenze **che una loro compromissione potrebbe provocare al sistema Paese.**



STRATEGICI

Dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale.

Non adatto a CSP a meno che non sia PSN Managed.



CRITICI

Dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese.



ORDINARI

Dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

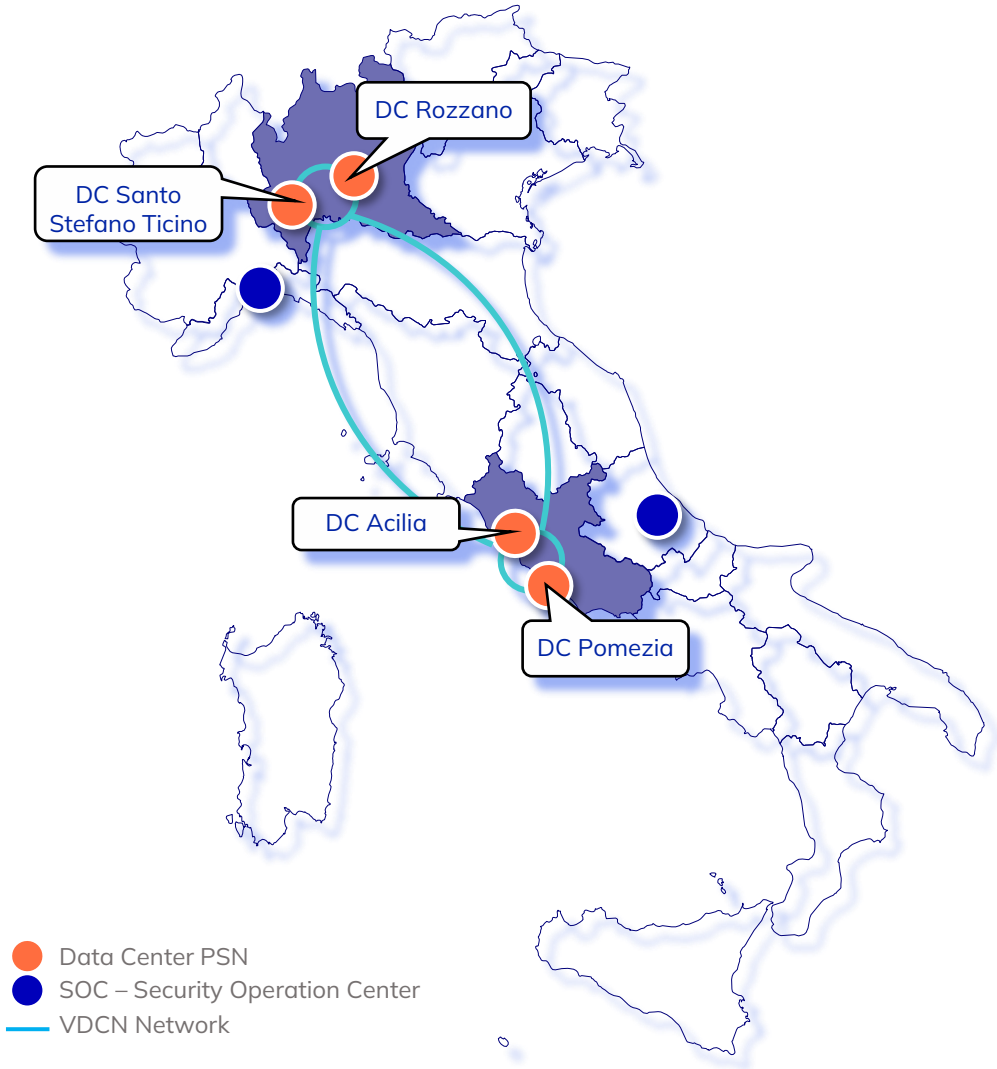
Agenda

1. INTRODUZIONE
2. CONTESTO DI RIFERIMENTO
3. I VALORI DI POLO STRATEGICO NAZIONALE
   - L’infrastruttura: garanzia di efficienza e resilienza
   - La sicurezza al centro delle attività di PSN
   - Le certificazioni
   - I vantaggi di Aderire a PSN
   - Il nostro percorso vero un obiettivo ambizioso
4. SOLUZIONI OFFERTE DA POLO STRATEGICO NAZIONALE
5. COME ADERIRE



L'infrastruttura di Polo: garanzia di efficienza e resilienza

Il cardine di Polo Strategico Nazionale è un'infrastruttura in linea con **i più elevati standard tecnologici**, con logiche integrate di funzionamento per garantire affidabilità, resilienza e disaster recovery.



4 Data Center in doppia region Milano e Roma
Garantiscono continuità operativa e disaster recovery

Sicurezza fisica dei Data Center
I Data Center sono protetti da diversi livelli di sicurezza fisica

Connettività intra-region 100Gbs
Connessioni a doppio anello, su doppia via

Security Operation Center (SOC)
Come operativo per la cybersecurity di Leonardo, opera 24h per proteggere le infrastrutture strategiche italiane

Computer Emergency Response Team (CERT)
Per intervenire immediatamente in caso di incidenti e prevenirli

La sicurezza al centro delle attività di PSN

Lo scopo di Polo Strategico Nazionale è quello di dotare la Pubblica Amministrazione Italiana di una struttura nazionale efficiente, affidabile e resiliente. La risposta alle sfide poste alla PA risiede in un concetto: **la sicurezza**.

SICUREZZA A 360°

Con l'infrastruttura nazionale e un solido sistema di operations, Polo Strategico Nazionale garantisce la **sicurezza in 3 ambiti fondamentali**

SICUREZZA INFORMATICA

- **Protezione dei dati** da attacchi informatici h24.
- **Conservazione dei dati** e **resilienza** da eventi ambientali
- **Indipendenza** da aziende Extra-EU nella gestione dei dati, gestiti solo nel territorio nazionale, criptati e securizzati all'interno del Paese.

SICUREZZA FISICA DEI DATA CENTER

- Data Center protetti da molteplici e diversificati **livelli di sicurezza fisica**
- Alti standard di **sicurezza dei campus** che ospitano i Data Center

SISTEMA DI GOVERNANCE

- Sistema di **governance della sicurezza**, promuovendo efficienza ed efficacia della sicurezza dei servizi Cloud
- Le Matrici di Responsabilità Condivisa della Sicurezza

Massima protezione dei dati della Pubblica Amministrazione, massima sicurezza per i cittadini

La sicurezza al centro delle attività di PSN

Le misure di sicurezza adottate da PSN garantiscono la **protezione dei dati da attacchi informatici**, sempre più frequenti ed evoluti, **la sovranità dei dati**, gestiti all'interno del territorio nazionale e la **resilienza ed affidabilità nella conservazione**.

Infrastruttura nazionale

I 4 data center su territorio italiano, garantiscono **autonomia tecnologia** del Paese richiesta dall'ACN e dall'UE.



La presenza **Dual Region** garantisce **business continuity e resilienza**, con DC basati su zone **a basso rischio di disastri** ambientali

Securizzazione Multicloud

PSN offre un servizio Multicloud con i principali Cloud Service Provider esteri, garantendo la crittografia dei dati e la securizzazione all'interno dei confini nazionali all'interno dei 4 Data Center in Italia.

Security Operation Center

Il centro di eccellenza di Leonardo, localizzato a Chieti e Genova, che lavora h24, 7 giorni su 7, per proteggere le infrastrutture strategiche per il Paese.

LEONARDO

Data Protection System

Sistema self-managed per Back up e ripristino dati. Articolato in 3 flussi:

» **Back up**
Può essere effettuato sia presso i DC PSN sia sui Public Cloud. Prevede una seconda copia dei dati in una seconda zona della Region.

» **Golden Copy**
Copia dei dati una Region differente, **nel** formato WORM, incancellabile e inalterabile. Intercetta malware che potrebbero compromettere il restore.

» **Disaster recovery**
Ripristino della struttura IT della PA dopo eventi disastrosi, grazie all'allineamento dei dati della PA in una Region diversa dal sito primario.

La sicurezza al centro delle attività di PSN

Oltre a garantire la sicurezza informatica, PSN garantisce la protezione fisica dei Data Center e un sistema di gestione interno per definire le responsabilità sulla sicurezza dei servizi.

SICUREZZA FISICA DEI DATA CENTER

I Campus che ospitano i Data Center di TIM garantiscono la massima resilienza, affidabilità ed efficienza delle strutture, certificata a livello internazionale.

I Data Center sono protetti da più livelli di sicurezza garantendo la protezione dei dati al loro interno

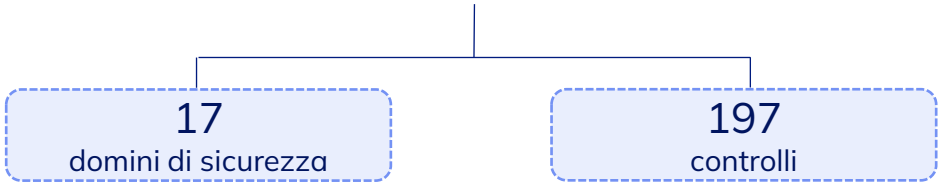
- recinzioni esterne ed interne, presidio di vigilanza armata
- recinzione perimetrale anti-scavalcamento
- sistema perimetrale di rilevazione antintrusione
- sistema integrato di videosorveglianza
- ronde di sorveglianza interne ed esterne
- vetri perimetrali blindati
- tornelli di sicurezza per l'accesso pedonale
- bussole di sicurezza sull'accesso alle sale sistemi

In coerenza con il framework del Cloud Service Alliance (CSA), PSN ha definito un sistema di gestione delle responsabilità dei Servizi Cloud

Matrici di Responsabilità Condivisa della Sicurezza

definiscono in trasparenza e chiarezza, la suddivisione delle responsabilità dei servizi Cloud tra Polo Strategico Nazionale e le Amministrazioni clienti

Cloud Control Matrix



Per ognuno dei controlli vengono accertate:
- l'applicabilità o meno di quello specifico requisito
- La responsabilità, al fine di individuare l'owner del controllo, se è di PSN, della PA o condiviso.

Le certificazioni

CSA (Cloud Security Alliance)

- **CSA Star Level 2** tra le più importanti certificazioni sulla sicurezza informatica dei servizi cloud, che valuta il sistema di Gestione della Sicurezza delle Informazioni.

ACN (Agenzia per la Cybersicurezza Nazionale)

- **Qualifiche ACN:** i servizi di Polo Strategico Nazionale sono qualificati secondo gli standard richiesti dall'agenzia per la cybersicurezza nazionale

ISO (International Organization for Standardization)

- **ISO27001** sulla sicurezza delle informazioni, non solo informatica, ma anche logica, fisica e organizzativa.
- **ISO9001** definisce i principi di gestione della qualità.
- **ISO20000-1** sulla gestione dei servizi di Information Technology, in coerenza con le infrastrutture.
- **ISO22301:2019** a garanzia della business continuity

Certificazioni Data Center

I Campus possiedono le massime certificazioni sulla sicurezza infrastrutturale

ANSI/TIA-942 Rating 4

Certificazione specifica per i Data Center, che stabilisce 4 livelli di rating per valutare l'affidabilità di un Data Canter, basandosi suoi elementi costruttivi.

UPTIME INSTITUTE TIER III e IV

La certificazione verifica l'applicazione degli Uptime Institute's Tier Standards, standard che definiscono le performace dell'infrastruttura.

Oltre alla sicurezza dei dati, i Data Center garantisco anche un basso impatto ambientale garantito dalle certificazioni

Leed Gold e Leed Platinum
ISO50001 sistema di gestione dell'energia
ISO14001 sistemi di gestione ambientale

***NOTE** Vedere slide in n. 43 in Annex per dettagli sulla normativa in tema di sicurezza e n. 44 per dettagli sulle certificazioni ISO e le qualifiche ACN

I vantaggi di aderire a Polo Strategico Nazionale

Unico multicloud

PSN è **l'unico operatore Multicloud** in Italia, che permette di scegliere, oltre al **Cloud PSN** anche tra i **Cloud Service Provider** esperti (**GSP, AWS, Azure, Oracle**) ma garantiti e securizzati nel territorio Italiano

Continuità della gestione

Aderendo a PSN, le PA non migrano solo al Cloud, ma vengono **accompagnate in un percorso di 10 anni di Journey-in-the-Cloud**, potendo sempre contare sull'affidabilità ed esperienza dei professionisti PSN.

Finanziabilità delle risorse

La migrazione verso il cloud qualificato di PSN può essere **finanziabile mediante l'accesso ai fondi previsti dal PNRR**, portando un risparmio dei costi di gestione dei DC e uno snellimento dei processi.

Polo Strategico Nazionale

Innovazione tecnologica

PSN offre a ogni PA, una vasta gamma di servizi innovativi, **le migliori soluzioni tecnologiche** per le infrastrutture di Data Center, piattaforme, Servizi Cloud e Cybersecurity.

Sicurezza e qualità dei servizi

I dati e servizi delle PA sono gestititi all'interno di **Data Center nazionali**, che garantiscono alti standard di **sicurezza fisica e informatica**, certificata. La Dual Region garantisce **ridondanza e resilienza.**

Efficienza e sostenibilità

La gestione dei 4 Data Center nazionali garantisce un impatto positivo sulla **spesa pubblica** e **sull'efficientamento energetico**, comprovato dalle certificazioni ISO 50001, ISO 14001, LEED Gold.

Il percorso e le milestone

24 Agosto 2022

La Convenzione ✓

Polo Strategico Nazionale sottoscrive la **Convenzione con il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri,** per la durata di 13 anni.

Le singole Amministrazioni posso stipulare **Contratti di Utenza** con PSN.

22 Dicembre 2022

Il Collaudo ✓

Attivato il Polo Strategico Nazionale attraverso la finalizzazione della fase di **collaudo e l'asseverazione dell'infrastruttura**, in accordo con le scadenze fissate dalla Concessione e dalla milestone del PNRR.

Settembre 2024

Prima Milestone ✓

A settembre 2024 è stata **raggiunta la prima milestone** prevista dal progetto:

- Avere almeno **100 Amministrazioni**, con almeno **un servizio migrato** sull'infrastruttura PSN

PSN ha raggiunto e **superato** la Prima Milestone con un totale di:

238 PA con servizio strategico migrato

206 PA Asseverate

Giugno 2026

Seconda Milestone

Entro Giugno 2026 è fissata la **seconda milestone** prevista dal progetto:

- Avere almeno **280 Amministrazioni**, con il 40% dei servizi migrati sull'infrastruttura PSN

Febbraio 2027

Adesione

La **chiusura della finestra di adesione** è stata fissata a **Febbraio 2027**

*«Vogliamo **abilitare l'innovazione e la trasformazione digitale** italiana attraverso la **gestione sicura dei dati e dei servizi** della Pubblica Amministrazione»*

Polo Strategico Nazionale

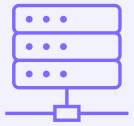
Polo Strategico Nazionale

Agenda

1. INTRODUZIONE
2. CONTESTO DI RIFERIMENTO
3. POLO STRATEGICO NAZIONALE: PERCORSO, VANTAGGI E TECNOLOGIE
4. LE SOLUZIONI OFFERTE
   - Servizi dedicati a ogni esigenza della PA
   - Modalità di migrazione
   - Servizi di infrastruttura tradizionali
   - Servizi di Private cloud
   - Servizi cloud con Cloud Service Provider
   - Soluzioni cloud per ogni livello di classificazione dei dati
   - Servizi Professionali per accelerare il «journey to cloud»
   - Ampliamento del listino
   - Modalità di acquisto dei servizi di Polo Strategico Nazionale
5. COME ADERIRE



Modalità di acquisto dei servizi di Polo Strategico Nazionale



I servizi **di Private Cloud** sono acquistabili nelle quantità previste con un **canone annuale fatturato con cadenza bimestrale** a seguito del set-up infrastrutturale



I **servizi professionali** sono acquistabili nelle quantità previste con una **tariffa giornaliera fatturata con cadenza bimestrale** a stato avanzamento lavori



I **servizi CSP** sono acquistabili nelle quantità previste con una **tariffa a consumo fatturata con cadenza bimestrale** a seguito del set-up infrastrutturale



I **pagamenti** sono previsti **a 30 giorni** dall'emissione della fattura

Modalità e prezzi di acquisto dei servizi sono regolamentati dalla Convenzione.

Catalogo Servizi PSN, dedicati a ogni esigenza della PA

L'offerta è costruita per essere la più ampia possibile e permettere dunque ad ogni PA di scegliere le soluzioni più idonee alle proprie esigenze e alla propria classificazione di dati e servizi.

Servizi di Migrazione

- Re-Host
- Re-Platform
- Re-Architect

Servizi di Infrastruttura Tradizionali

- Housing
- Hosting

Servizi di Private Cloud

- IaaS Shared
- IaaS Dedicated
- PaaS
- CaaS
- Cloud Storage
- Data Protection

Servizi Cloud con Cloud Service Provider

- Public Cloud PSN Managed (PSN + Oracle/Google Cloud)
- Hybrid Cloud on PSN site (PSN + Microsoft Azure)
- Secure Public Cloud (PSN + Microsoft Azure /Google Cloud + AWS + Oracle)

Servizi Professionali

- Security Services & Compliance
- IT Infrastructure - Service Operations
- Business & Culture Enablement

Altri servizi

- Connettività
- Multicloud
- Antivirus
- Sistemi operativi

Servizi di migrazione

Offriamo diversi servizi aggiuntivi per accompagnare le Amministrazioni nel percorso di migrazione al Cloud verso il futuro digitale. I Servizi Professionali per la migrazione, consistono in una serie di attività funzionali che arrivano fino dalla riprogettazione completa delle applicazioni della PA.

STRATEGIA DI MIGRAZIONE

Livello di complessità

Re-Host

Le soluzioni **Re-Host** sono servizi professionali per la migrazione veloce delle piattaforme AS-IS (Lift & Shift), che ospitano le applicazioni della **Pubblica Amministrazione.**

Re-Platform

Le soluzioni **Re-Platform** sono servizi professionali evolutivi per la riprogettazione delle piattaforme che ospitano le applicazioni della Pubblica Amministrazione, allo scopo di abilitarne la trasformazione verso il cloud.

Re-Architect

Le soluzioni di **Re-Architect** sono servizi professionali evolutivi ideati per la riprogettazione dell'architettura delle applicazioni in ottica cloud.

Modalità A
Journey to the cloud
Trasferimento in sicurezza dell'infrastruttura IT
APPROFONDIMENTI

Modalità B
Journey in the cloud
Aggiornamento di applicazioni sicure in Cloud
APPROFONDIMENTI

Servizi di infrastruttura tradizionali

Polo Strategico Nazionale mette a disposizione della Pubblica Amministrazione italiana servizi di Housing e Hosting, con l'obiettivo di fornire soluzioni infrastrutturali tradizionali sicure ed efficienti.

Housing: uno spazio nei Data Center PSN

Scegliendo l'**Housing**, le Amministrazioni utilizzano uno spazio attrezzato di proprietà di Polo Strategico Nazionale.
Con questo servizio la PA si garantisce uno **spazio fisico all'interno dei DC di PSN**.
Polo Strategico Nazionale si occuperà delle attività di gestione e potrà fornire ulteriori servizi aggiuntivi a supporto della PA.



Hosting: utilizzo dei server PSN

Optando per l'**Hosting**, le **Amministrazioni** hanno la possibilità di **utilizzare server dedicati** di proprietà di Polo Strategico Nazionale per ospitare le proprie applicazioni. PSN si occuperà della gestione dell'infrastruttura e della sicurezza.
Il servizio di Hosting garantisce l'interconnessione con i sistemi della PA presenti nelle altre tipologie di servizi erogati alla stessa da Polo Strategico Nazionale.

Servizi di Private Cloud (1/4)

Polo Strategico Nazionale mette a disposizione della Pubblica Amministrazione servizi di Private Cloud.
Si tratta di soluzioni *on demand* e *as a service* su infrastrutture virtualizzate e piattaforme per la gestione degli applicativi, che rispondono a diverse esigenze delle Amministrazioni italiane.



IaaS Shared
(Infrastructure as a Service)

IaaS Shared di Polo Strategico Nazionale è un servizio in cui l'infrastruttura (computing, storage e networking) è virtualizzata e viene erogata attraverso **risorse computazionali logicamente segregate** tra di loro, per garantire la sicurezza della singola pubblica amministrazione rispetto alle altre.



IaaS Dedicated
(Infrastructure as a Service)

IaaS Dedicated di Polo Strategico Nazionale è un servizio in cui l'infrastruttura (computing, storage e networking) è virtualizzata e viene erogata attraverso **risorse computazionali dedicate e segregate tra di loro**, per garantire la sicurezza della singola pubblica amministrazione.



PaaS
(Platform as a Service)

PaaS è un servizio che prevede la messa a disposizione di una o più piattaforme tecnologiche in cloud (logicamente o fisicamente segregate), che permettono di sviluppare ed erogare elementi applicativi (IAM, Big Data, Artificial Intelligence) e di middleware (Database).
Tali piattaforme così come le infrastrutture su cui si basano sono gestite end-to-end da PSN.



CaaS
(Container as a Service)

CaaS di Polo Strategico Nazionale è un servizio che permette di creare, distribuire, gestire applicazioni e dati utilizzando il modello, "cloud native", basato su container dove, PSN, mette a disposizione anche la relativa piattaforma di orchestrazione.



Cloud Storage

Soluzioni ad-hoc per la gestione dei dati offerti da Polo Strategico Nazionale. Il cloud storage è un **servizio di archiviazione dati basato su cloud** che consente agli utenti di memorizzare, gestire ed accedere ai propri dati ridondati, geograficamente replicati.



Data Protection

Il servizio di Data Protection è un servizio che consente di eseguire il **backup** dei contenuti informativi conservati in cloud (eventualmente anche con la feature della **Golden Copy**).
Permette inoltre di progettare soluzioni di **Disaster Recovery** personalizzate.

Servizi di Private Cloud – PaaS (2/4)

Il servizio Industry Standard PaaS mette a disposizione delle PPAA una piattaforma in grado di erogare component di *middleware* secondo un modello a servizio, astraendo l'infrastruttura sottostante.
PSN è responsabile dell'infrastruttura sottostante comprensiva sia di strumenti di *automation* e *orchestration* che dei servizi di piattaforma. Il PaaS di Polo Strategico Nazionale si compone dei seguenti sottoservizi:

PaaS DB
(Database as a Service)

Consente alle PPAA di **configurare e gestire database** senza preoccuparsi dell'infrastruttura sottostante.
PSN è responsabile di tutto **lo stack d'infrastruttura** comprese le operazioni di riconfigurazione, della capacità elaborativa, del backup e delle repliche intra-region.

IAM
(Identity Access Management Spid Enabling & Profiling)

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

Big Data
(Data Lake)

Il servizio consente la costruzione di **Data Lake as a service**, ovvero un archivio di dati che permette di immagazzinare grandi volumi di informazioni strutturate e non strutturate, provenienti da fonti diverse. La soluzione inoltre permette l'uso di strumenti di analisi avanzata come l'apprendimento automatico e l'intelligenza artificiale per estrarre informazioni di interesse.

AI
(Artificial Intelligence)

Polo Strategico Nazionale mette a disposizione un **set di algoritmi pre-addestrati** di Artificial Intelligence per utilizzarli ad esempio per analisi del testo piuttosto che analisi di audio/video. Inoltre è disponibile una piattaforma per la realizzazione di modelli custom di machine/deep learning.

Servizi di Private Cloud - Cloud Storage (3/4)

Polo Strategico Nazionale mette a disposizione della Pubblica Amministrazione dei servizi di Cloud Storage. Si tratta di soluzioni *on demand*, che consentono agli utenti di memorizzare, gestire e accedere ai propri file e dati geograficamente distribuiti.



High Performance

Una **SAN** (Storage Area Network) **basata su NVMe** (Non-Volatile Memory Express), ovvero un'infrastruttura di storage ad alte prestazioni che utilizza la tecnologia NVMe per consentire un'archiviazione veloce e a bassa latenza. NVMe è un protocollo di comunicazione che **ottimizza l'accesso ai dispositivi di storage basati su memoria flash**, offrendo prestazioni superiori rispetto alle tradizionali tecnologie di storage (170.000 IOPS).



Standard Performance

Una **SAN** (Storage Area Network) **basata su tecnologia All Flash**, replicata intra-region, con una capacità di 130.000 IOPS (Input/Output Operations Per Second) per Storage Array, offre un'infrastruttura di storage ad alte prestazioni che **utilizza dispositivi di storage completamente a stato solido (SSD)** per fornire velocità e prestazioni elevate (130.000 IOPS).



High e Standard Performance Encrypted

Le tecnologie per queste due tipologie di storage sono le medesime descritte per High e Standard performance in aggiunta a questo, viene fornito un servizio di **crittografia a livello di singolo volume.** La crittografia a livello di singolo volume **garantisce che ogni volume di storage sulla SAN venga crittografato separatamente**, utilizzando algoritmi crittografici robusti e sicuri. La crittografia assicura che il **dato sia indecifrabile da chi non autorizzato** a farlo ed in possesso della chiave che ne decodifichi il contenuto.



Network Attached Storage (NAS)

NAS (Network Attached Storage) è una soluzione di archiviazione di dati che **consente agli utenti di memorizzare, gestire e condividere file** su una rete locale. A differenza dei dispositivi di storage interni al computer**, un NAS è un dispositivo autonomo collegato alla rete** che fornisce spazio di archiviazione centralizzato accessibile da più dispositivi, come computer, server, dispositivi mobili e altri dispositivi connessi alla rete.



Object Storage

Object storage è un modello di archiviazione dei dati che **organizza i file in "oggetti" indipendenti** con un identificatore univoco chiamato "chiave". A differenza del tradizionale modello di archiviazione basato su file system, dove i dati sono organizzati in una struttura gerarchica di directory e file, l'object storage **memorizza i dati come oggetti separati con metadati associati**. Tali oggetti sono accessibili tramite API (Application Programming Interface).

Servizi di Private Cloud - Data Protection (4/4)

Il servizio Data Protection mette a disposizione della PA delle soluzioni sicure per la conservazione dei propri dati. Il servizio di Backup si integra con il disegno infrastrutturale di PSN basato su zone di disponibilità in «Region» geograficamente distribuite. Su richiesta può essere attivata un'ulteriore copia secondaria di backup (Golden Copy), non cancellabile ed inalterabile. Inoltre con l'opzione DR le PA possono costruirsi il proprio servizio di Disaster Recovery geograficamente distribuito sulle «Region» di PSN.

Backup

Tramite **un'unica console centralizzata** gli utenti della PA potranno **gestire in autonomia** la protezione dei dati presenti sia sui Data Center PSN che sui Public Cloud (Hybrid/Secure/Managed). I dati di backup potranno essere **storicizzati sia presso i Data Center PSN che presso i relativi Cloud Storage dei Public Cloud dove risiedono**. Il servizio di backup/restore, garantirà all'utente totale autonomia sia per il salvataggio che per il recupero dei propri dati, permettendo il ripristino ad una certa data.

Golden Copy

Quale **ulteriore elemento di garanzia della protezione dei dati**, oltre al backup, PSN mette a disposizione un servizio opzionale aggiuntivo che **analizza i backup** allo scopo di **intercettare eventuali contaminazioni da malware silenti**, che comprometterebbero la validità di un eventuale restore in produzione. 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** (AIR-GAP: Isolation, WORM: Write Once, Read Many, Ransomware Protection).

Opzione DR

Il Disaster Recovery è il servizio di cloud computing che **consente il ripristino dei servizi** sottoscritti a seguito di **un evento disastroso**. Tale opzione viene erogata self-managed da parte della PA che può sfruttare architetture di DR standard predefinite e securizzate. **Tale servizio si basa sulla replica dello storage** e sugli automatismi che permettono l'allineamento delle risorse delle **PA in una region di PSN diversa** dall'ubicazione primaria.

Servizi Cloud con Cloud Service Provider

Grazie a Polo Strategico Nazionale, la PA può accedere ai servizi CSP con elevati livelli di sicurezza, protezione e controllo del dato, in funzione dei propri bisogni e in modalità *managed*, *public* e *hybrid*. I servizi, attualmente sono realizzati in partnership con AWS, Oracle, Google e Azure, in futuro potranno essere erogati anche con altri Cloud Service Provider. Tutti i servizi sono integrati con infrastrutture di *external key management* e con servizi di *backup by design*.

Public Cloud PSN Managed
(PSN + Oracle)

Servizi erogati **su region italiane e/o su infrastrutture di proprietà di Polo Strategico Nazionale**, operati e controllati da personale di Polo Strategico Nazionale, con separazione logico-fisica dalla parte pubblica del CSP.

- Separazione delle componenti, in particolare tra parte Cloud dedicata e pubblica
- Gestione del full stack (dall'hardware alla piattaforma software) erogata da personale PSN altamente qualificato
- Gestione di tutte le fasi, dal rilascio del software alla gestione hardware e replacement, con distruzione dischi in fase di sostituzione
- Controllo della Root Key (coppia di chiave pubblica + chiave privata associata a un dispositivo) della region
- Erogazione servizi in modalità completamente disconnessa dalle region pubbliche del Cloud Service Provider

Hybrid Cloud on PSN site
(PSN + Microsoft Azure)

Servizi erogati tramite **infrastruttura proprietaria di Polo Strategico Nazionale**, che prevedono una **combinazione di cloud pubblico e privato**.

- Gestione centralizzata e integrata con dati su perimetro fisico gestito da Polo Strategico Nazionale (inclusi backup e DR)
- Erogazione di servizi IaaS & PaaS equivalenti a quelli su Azure Public Cloud (Kubernetes, SQL Data Services, Azure VM...)
- Utilizzo innovativo del cloud con un'estensione delle capabilities verso sistemi on premises
- Control plane unico con Azure Arc
- Servizi di sicurezza on premise PSN (SOC e CERT) e l'integrazione con soluzioni di Key Management on premise PSN

Secure Public Cloud
(PSN + Microsoft Azure/Google Cloud/AWS/Oracle)

Servizio localizzato **sulle region italiane dei CSP, securizzato** utilizzando chiavi di crittografia di Polo Strategico Nazionale.

- Gestione delle chiavi di crittografia esterna al perimetro di controllo del CSP
- Garantita security by policy/design creando per ogni cliente un ambiente standard segregato e auto-consistente
- Confidential computing, rende impossibile agli operatori del cloud provider di accedere al dato in uso garantendo la data sovereignty
- Soluzione Hub & Spoke garantisce che tutto il traffico di rete possa essere controllato e monitorato
- Possibilità di mantenere una copia dei dati su infrastruttura PSN, a supporto della protezione, resilienza e recuperabilità del dato

Servizi Professionali

Servizi professionali opzionali che le PPAA possono acquistare per la gestione operativa, della sicurezza e dell'infrastruttura IT, messa a disposizione da Polo Strategico Nazionale.

Security Services & Compliance

I Security Services & Compliance sono progetti di **Strategy & Compliance**, finalizzati a valutare la **sicurezza di un'infrastruttura** e il suo parco applicativo, oltre che per dare supporto al mantenimento degli elevati standard di sicurezza delle Amministrazioni.

La **protezione delle informazioni della Pubblica Amministrazione** è prioritaria per Polo Strategico Nazionale, che mette a disposizione una serie di strumenti volti non solo a garantirla ma anche a controllarla nel tempo, offrendo un sostegno al cliente in tutte le fasi di transizione digitale.

IT Infrastructure - Service Operations

L'IT Infrastructure è un gruppo di servizi specialistici on demand a supporto delle Operations per la gestione dell'infrastruttura e del parco applicativo della **Pubblica Amministrazione**.

Sono **Service Operations** che vengono erogati da un personale con ampia esperienza nella gestione operativa dei Data Center e di contesti virtuali nei vari modelli di servizio.

Business & Culture Enablement

I servizi **Business & Culture Enablement** abilitano sinergicamente la cultura organizzativa necessaria alla trasformazione digitale della PA:

- **Change Management:** organizzazioni e persone vengono accompagnate nell'utilizzo ottimale di risorse, conoscenze e strumenti per la trasformazione digitale;
- **Formazione:** un'apposita piattaforma e-Learning eroga un'offerta completa di corsi base a catalogo e/o personalizzati su tematiche specifiche;
- **Supporto Specialistico:** un portfolio di figure professionali favorisce un'ulteriore accelerazione del processo di trasformazione digitale delle Amministrazioni.

Altri servizi

PSN mette a disposizione delle PA una serie di servizi aggiuntivi a completamento dell'offerta, che vanno dalla connettività dedicata abilitante le fasi di migrazione alla gestione dei *workload* in ambienti *multicloud* offerti da PSN, fino alla fornitura di servizi di gestione antivirus *end-to-end* per ambienti complessi. Sono inoltre disponibili sistemi operativi di tipo *licenced*. Di seguito una breve descrizione dei servizi sopra citati:



Connettività

La **connettività** offerta da PSN è una **connessione dedicata ad 1 Gbps** utilizzabile temporaneamente durante le fasi di migrazione delle applicazioni e dei dati. Tale servizio consiste nella fornitura dedicata con terminazione nel Data Center di erogazione dei servizi PSN.



Multicloud

A completamento dell'offerta dei servizi Cloud proposti, **PSN offre la possibilità di integrarsi** con le soluzioni di Public Cloud dei principali player e Cloud Provider internazionali. L'offerta **Multicloud** si propone come **soluzione completa** per la gestione di architetture Hybrid & Multicloud anche attraverso l'utilizzo di un'unica Cloud Management Platform che ne semplifica la gestione.



Antivirus

Tale offerta consiste nella fornitura di un **servizio Fully Managed EDR/Antivirus**, con relativo controllo centralizzato di tutte le componenti in ambito per proteggere in modo specifico gli ambienti IT delle Amministrazioni.



Sistemi Operativi

Tale servizio consiste nella fornitura alle Amministrazioni **di licenze di sistemi operativi** Windows e Linux Red Hat (ultima release disponibile).

Polo Strategico Nazionale

2.

Servizi di migrazione



Servizio di migrazione Re-Host

La migrazione di tipo «Re-Host» in ambito cloud è un approccio mediante il quale un'applicazione o un sistema software viene trasferito da un'infrastruttura on-prem ad un ambiente cloud attraverso una modalità di moving strettamente infrastrutturale, senza la necessità di apportare modifiche all'applicazione stessa.

Tale approccio anche conosciuto come «Lift & Shift», è basato sulla facilità e sulla velocità di migrazione, consentendo alle organizzazioni di beneficiare rapidamente delle funzionalità offerte dal cloud, come la scalabilità, l'affidabilità e l'elasticità, senza dover dedicare tempo e risorse per ridisegnare o riscrivere l'applicazione.

Vantaggi:

- **Velocità di migrazione**: il Re-Host consente di migrare rapidamente le applicazioni esistenti nel cloud senza dover apportare modifiche significative al codice o all'architettura. Ciò riduce il tempo e lo sforzo necessari per portare le applicazioni nell'ambiente cloud.
- **Minore complessità**: evitando modifiche sostanziali all'applicazione, il Re-Host riduce la complessità del processo di migrazione. Non è necessario riscrivere o ridisegnare l'applicazione, ma solo trasferire l'intera infrastruttura esistente nell'ambiente cloud.
- **Utilizzo delle funzionalità cloud**: anche se l'applicazione non sfrutta appieno le funzionalità native del cloud, il Re-Host consente comunque di beneficiare di alcune caratteristiche, come la scalabilità orizzontale, l'affidabilità del servizio e la gestione semplificata delle risorse.
- **Riduzione dei costi**: la migrazione al cloud mediante il Re-Host può ridurre i costi operativi, eliminando la necessità di gestire e mantenere l'infrastruttura locale. Inoltre, i modelli di pagamento basati sul consumo offerti dai fornitori di servizi cloud consentono di pagare solo per le risorse effettivamente utilizzate.
- **Processo Industrializzato**: tale migrazione risulta facilmente automatizzabile, replicabile e industrializzata, grazie alla disponibilità di framework, tools, metodologie disponibili e consolidate sul mercato per ogni tipologia di migrazione e per ogni tipologia di target (Private o CSP).

Servizio di migrazione Re-Platform

La migrazione di tipo «Re-Platform» si applica nei casi in cui per sfruttare al meglio i servizi cloud è richiesta la modifica di alcune componenti tecnologiche di un'applicazione, in modo tale da renderli compatibili con i requisiti minimi di portabilità.

Tale approccio può prevedere upgrade, cambi tecnologici, modifiche dell'architettura e riguarda principalmente i layer relativi ai Sistemi Operativi, ai Database, agli Application server ed in generale a tutte quelle categorie definite come «middleware» (es: API, EAI, ETL...).

La migrazione Re-Platform può essere considerata come un passaggio intermedio prima di adottare soluzioni più avanzate, che implicano la riscrittura o la reingegnerizzazione delle applicazioni.

Vantaggi:

- **Ottimizzazione delle risorse e dei costi**: permette di utilizzare le caratteristiche dell'infrastruttura cloud senza richiedere modifiche significative agli applicativi con l'obiettivo di mantenere il codice il più invariato possibile. Ciò significa che il codice sorgente viene riutilizzato o solo leggermente modificato per adattarsi all'ambiente di destinazione.
- **Tempi di migrazione contenuti**: la migrazione di tipo Re-Platform richiede meno sforzo rispetto ad altre strategie di migrazione più complesse, come la riscrittura completa o la reingegnerizzazione delle applicazioni. Questo consente di risparmiare tempo e risorse preziose durante il processo di migrazione.
- **Utilizzo di servizi cloud native**: rispetto ad una migrazione di tipo Re-Host permette di sfruttare e/o integrare in modo più semplice i servizi PaaS messi a disposizione dai Cloud Service Provider.

Servizio di migrazione Re-Architect

La migrazione di tipo «Re-Architect» ha come obiettivo quello di trasformare le applicazioni delle PA secondo il paradigma cloud-native sfruttando al meglio tutti i servizi cloud offerti da PSN. Questo permette di modernizzare i servizi che le PA offrono e al contempo aumentare i livelli di sicurezza, resilienza, scalabilità e performance delle applicazioni stesse.

Tale tipo di trasformazione richiede sicuramente maggior impegno in termini di tempo e di effort, ma è quella che produce il maggior valore sia da un punto di vista della qualità dei servizi che di digitalizzazione dei relativi processi che di innovazione.

Vantaggi:

- **Incremento della sicurezza** grazie alla possibilità di evolvere le applicazioni secondo approcci Secure by design;
- **Ottimizzazione dell'architettura applicativa** per sfruttare al meglio le caratteristiche del cloud in termini di disponibilità, scalabilità, osservabilità, resilienza, provisioning delle risorse e della sicurezza;
- **Possibilità di utilizzo di metodologie** di test consolidate e automatizzate per le verifiche funzionali, di qualità e di sicurezza;
- **Allineamento alle best practices** di mercato per lo sviluppo e la progettazione, che consentono la trasformazione del codice applicativo in modo controllato;
- **Modernizzazione dell'applicazione** che permette un riuso e maggior velocità per implementare eventuali ulteriori evoluzioni.

Fasi della migrazione

Per la gestione operativa della migrazione, in linea con quanto definito nella Relazione Tecnico Illustrativa della documentazione contrattuale, sarà adottata una metodologia basata sul framework EMG2C (Explore, Make, Go to Cloud), articolato in tre distinte fasi:

EXPLORE	1. Analisi/Discovery	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	2. Setup 3. Migrazione	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 TO CLOUD	4. Collaudo	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.

Modalità A - Trasferimento in sicurezza dell'infrastruttura IT

L'opzione di Trasferimento in sicurezza dell'infrastruttura IT consente di sfruttare la strategia di migrazione Re-Host (anche detta Lift & Shift), cioè la migrazione al Cloud dell'infrastruttura già esistente, senza la necessità di reingegnerizzare le applicazioni.

Di seguito alcuni use case in cui l'approccio del Re-Host, può essere appropriato per la migrazione delle applicazioni al cloud:

1. Migrazione di un'applicazione web:

Si immagini di avere un'applicazione web esistente ospitata in un server on-premise. L'organizzazione potrebbe optare per il Re-Host al fine di migrare l'intera applicazione, inclusi i file di configurazione, i database e le risorse di sistema, in un ambiente cloud senza apportare modifiche significative al codice sorgente. Ciò consentirebbe di beneficiare dei vantaggi del cloud come la scalabilità e l'affidabilità senza dover riscrivere o ridisegnare l'applicazione.

2. Trasferimento di un sistema ERP:

In caso di un sistema ERP (Enterprise Resource Planning) installato localmente, il Re-Host potrebbe essere una scelta appropriata per migrare l'intero sistema nel cloud. In questo caso, è possibile sollevare e spostare l'infrastruttura ERP, inclusi i server, i database e le integrazioni di sistema, in un ambiente cloud senza apportare modifiche sostanziali al codice o all'architettura del sistema.

3. Migrazione di un'applicazione legacy:

In caso di un'applicazione legacy che è ancora vitale per le operazioni aziendali, ma i server o l'infrastruttura sottostante sono diventati obsoleti o richiedono un aggiornamento costoso, il Re-Host può offrire una soluzione rapida ed efficiente. È possibile migrare l'intera applicazione legacy nel cloud, mantenendo intatto il codice e riducendo i costi operativi legati all'infrastruttura on-premise.

4. Spostamento di un'applicazione di sviluppo e test:

Le organizzazioni che desiderano creare un ambiente di sviluppo e test nel cloud possono utilizzare l'approccio Re-Host per migrare l'intera infrastruttura di sviluppo e test. Questo consente di creare rapidamente un ambiente scalabile nel cloud senza dover modificare l'architettura dell'applicazione.

5. Consolidamento di data center:

In caso di organizzazioni con più data center distribuiti in diverse posizioni geografiche, il Lift & Shift può essere utilizzato per consolidare l'infrastruttura in un unico ambiente cloud. Ciò semplifica la gestione e riduce i costi operativi associati alla gestione di più data center fisici.

Modalità B - Aggiornamento di applicazioni sicure in Cloud

L'opzione di aggiornamento di applicazioni sicure in Cloud offre la possibilità di migrare le applicazioni utilizzando le strategie di Re-Platform e/o Re-Architect. Dove per replatforming, si intende la riorganizzazione dell'architettura applicativa sostituendo intere componenti del servizio, mentre per rearchitecting si intende un processo in cui un'applicazione o un sistema esistente viene riprogettato e ristrutturato, per sfruttare appieno le funzionalità native e le migliori pratiche offerte dal cloud.

Di seguito alcuni use case in cui l'approccio Re-Platform/Re-Architect, può essere appropriato per la migrazione delle applicazioni al cloud:

1. Aggiornamento del database:

Se l'applicazione dipende da un database obsoleto o che richiede un aggiornamento, il **replatforming** può essere una soluzione. Si può migrare l'applicazione su un ambiente cloud che supporta le versioni più recenti del database, senza dover riscrivere o ridisegnare l'applicazione stessa.

2. Estensione delle funzionalità dell'applicazione:

Se la necessità e quella di ampliare le funzionalità di una applicazione senza dover riscrivere l'intero codice, il **replatforming** può essere utile. È possibile migrare l'applicazione su un ambiente cloud che offre servizi aggiuntivi o componenti preconfigurati, come l'integrazione di servizi di intelligenza artificiale o di analisi dei dati, per estendere le funzionalità dell'applicazione esistente.

3. Scalabilità e ridondanza:

Se un'applicazione avesse necessità di scalabilità dinamica per gestire picchi di carico o richiedesse una maggiore ridondanza per garantire l'affidabilità, il **rearchitecting** può essere una scelta adeguata. È possibile ridisegnare l'architettura dell'applicazione per sfruttare servizi cloud come l'auto-scaling, i bilanciatori di carico e la distribuzione geografica per gestire le richieste di traffico in modo efficace e garantire la disponibilità continua.

4. Modernizzazione dell'architettura:

In caso di un'applicazione legacy con un'architettura monolitica che rende difficile l'aggiornamento e l'introduzione di nuove funzionalità, il **rearchitecting** può aiutare a modernizzare l'architettura. È possibile adottare un'architettura a microservizi o serverless, suddividendo l'applicazione in componenti modulari che possono essere gestiti e scalati indipendentemente, facilitando l'aggiornamento e l'integrazione di nuove funzionalità.

Polo Strategico Nazionale



3.

Servizi di infrastruttura tradizionali

Industry Standard - Housing

Il Servizio Industry Standard «Housing» consiste nella messa a disposizione di aree esclusive all'interno dei Data Center di PSN, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi, dove PSN ne gestisce l'accesso, l'accompagnamento, il *networking* e la sicurezza perimetrale fisica e logica.

Servizi inclusi

- Rack dedicato al cliente (1,75 mq)
- Potenza elettrica standard certifica e garantita (3.5 kW/rack)
- Cabling per l'interconnessione dei sistemi ad alte prestazioni
- Accesso ad Internet condiviso
- Gestione prossimità (DC/Infrastruttura)
- Accesso al datacenter per il cliente finale con la possibilità di accompagnamento nei locali di propria competenza
- Sicurezza perimetrale fisica e logica H24 (DC, network, FW, DDOS)
- Service Management: gestione cliente tramite un team specializzato per il supporto costante e proattivo
- Customer Operation Support: supporto di primo livello H24 erogato dal service desk con ingaggio tramite self-ticket o numero verde



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection: backup, golden copy, BC/DR
- Rack aggiuntivi
- Potenza elettrica aggiuntiva (+1 kW)
- Banda aggiuntiva dedicata
- Estensione ad altri servizi PSN (Hosting, Private cloud, CSP, ...)
- Moving dei server

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

Industry Standard - Hosting

Il Servizio Industry Standard «Hosting» consiste nella messa a disposizione, da parte di PSN, di una infrastruttura computing dedicata, gestita da PSN sia da un punto di vista Infrastrutturale che di Sicurezza, in grado di ospitare le applicazioni della PA che necessitino di segregazione fisica e necessità di requisiti tecnici specifici della PA e del suo contesto applicativo.

Servizi inclusi

Tutti i servizi già compresi nell'Housing ed inoltre:

- Gestione Sistemistica: servizio H24 di secondo e terzo livello per la gestione dell'infrastruttura di hosting (Compute, Storage e Network) ivi compreso il relativo sistema operativo (free o licenced);
- Security Operation Center (SOC): gestione della sicurezza dell'infrastruttura fisica e del networking.



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Object storage, NAS, Block storage, Storage encryption
- Sistemi operativi Windows/Linux Red Hat
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection: backup, golden copy, BC/DR
- Antivirus
- Banda aggiuntiva dedicata
- Funzionalità di encryption con KMS esterno (BYOL or HYOL)

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

Polo Strategico Nazionale



4.

Servizi di Private Cloud

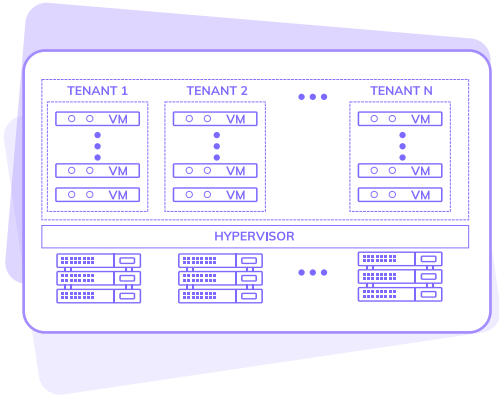
Industry Standard - IaaS Shared

Il Servizio Industry Standard «IaaS Shared» è un servizio cloud, in cui le risorse computing del cliente sono logicamente segregate e le relative configurazioni (VM o Pool, con o senza configurazione HA) vengono preattivate. PSN è responsabile della gestione completa dell'infrastruttura sottesa e delle piattaforme di virtualizzazione. Rende inoltre disponibile alle singole Amministrazioni gli strumenti e le console per la gestione in autonomia dei relativi ambienti per scalare le risorse a seconda delle necessità.

Servizi inclusi

Tutti i servizi già compresi nell'Hosting ed inoltre:

- Gestione Sistemistica: servizio H24 di secondo e terzo livello per la gestione dei layer di virtualizzazione (Compute, Storage e Network);
- Security Operation Center (SOC): gestione della Sicurezza dell'infrastruttura di virtualizzazione;
- Console di gestione con funzionalità abilitate a seconda dei profili.



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Object storage, NAS, Block storage, opzione standard o high performance, opzione encryption
- Sistemi Operativi Windows/Linux Red Hat
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection (backup, golden copy, DR)
- Opzione HA (business continuity)
- Antivirus
- Banda aggiuntiva dedicata
- Funzionalità di encryption con KMS esterno (BYOL or HYOL)

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

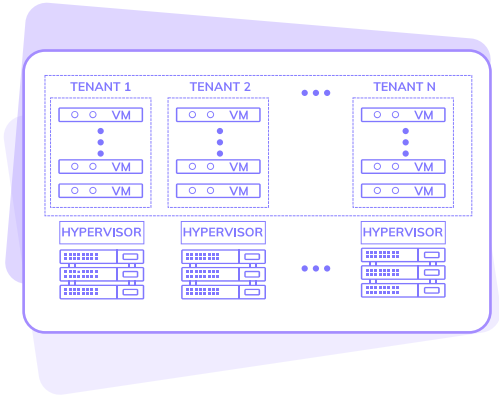
Industry Standard - IaaS Dedicated

Il Servizio Industry Standard «IaaS Dedicated» è un servizio cloud in cui le risorse computing del cliente sono segregate.
PSN è responsabile della gestione completa dell'infrastruttura sottesa e delle piattaforme di virtualizzazione. Rende inoltre disponibile alle singole Amministrazioni gli strumenti e le console per la gestione in autonomia dei relativi ambienti, per scalare le risorse a seconda delle necessità.

Servizi inclusi

Tutti i servizi già compresi nell'Hosting ed inoltre:

- Gestione Sistemistica: servizio H24 di secondo e terzo livello per la gestione dei layer di virtualizzazione (Compute, Storage e Network);
- Security Operation Center (SOC): gestione della Sicurezza dell'infrastruttura di virtualizzazione;
- Console di gestione con funzionalità abilitate a seconda dei profili.



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Object storage, NAS, Block storage, opzione standard o high performance, opzione encryption
- Sistemi Operativi Windows/Linux Red Hat
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection (backup, golden copy, DR)
- Opzione HA (business continuity)
- Antivirus
- Banda aggiuntiva dedicata
- Funzionalità di encryption con KMS esterno (BYOL or HYOL)

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

Industry Standard - PaaS DB

Il Servizio Industry Standard «PaaS DB» è un servizio cloud che mette a disposizione degli utenti finali un database in alta affidabilità per gestire dati in un ambiente virtualizzato senza la necessità di gestire l'infrastruttura sottostante. PSN mette a disposizione una vasta gamma di tecnologie di database SQL e non SQL, consentendo alle PA di utilizzare l'opzione più adatta alle proprie specifiche esigenze.



Servizi inclusi

Tutti i servizi già compresi nello IaaS Shared ed inoltre:

- Gestione Database: servizio H24 di secondo e terzo livello per la gestione dell'istanza di database, ivi compreso il monitoraggio, tuning e la modifica delle configurazioni del database;
- Security Operation Center (SOC): Gestione della Sicurezza fino all'istanza di database;
- Block storage (20 GB);
- Patching dell'engine.

Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Aggiunta di ulteriore Block storage, Storage encryption
- Data Protection (backup, golden copy, DR)
- Servizi professionali (es: migrazione, allineamento dati su istanze attive/passive, gestione degli schema/dati)

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

Industry Standard - PaaS IAM (Spid Enabling & Profiling)

Il servizio Industry Standard «PaaS IAM» è un servizio cloud che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano dentro PSN, affinché solo gli utenti autorizzati possano accedere alle risorse a loro assegnate. PaaS IAM coinvolge la gestione delle identità degli utenti, la creazione di ruoli e privilegi, l'accesso basato su regole e policy preassegnate, l'autenticazione multifattoriale e altre funzionalità di sicurezza. Tale servizio inoltre permette di semplificare l'integrazione tra servizi PSN e servizi esterni (on-prem, Spid).

Principali moduli funzionali disponibili all'interno del servizio IAM

Identity Management & Governance

- Componente responsabile nella gestione del ciclo di vita delle identità digitali, della creazione, modifica, cancellazione delle identità, dei loro attributi e del rapporto tra identità e attributi all'interno del sistema IAM
- Componente responsabile nella gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestire le risorse di amministrazione

Access Control Management

- Componente responsabile nella gestione dell'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali

Credential Management

- Componente responsabile nella gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.

Multi Factor Authentication

- Gestisce gli schemi di autenticazione utilizzati sul sistema IAM multi-fattore (gestione delle password, OTP Token, Smart Card, etc.)
- Per garantire la sicurezza dell'intera filiera applicativa il sistema di autenticazione multi-fattore deve garantire i livelli di sicurezza definiti all'interno della norma ISO/IEC DIS 29115

Logging & Reporting

- Componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema IAM per generare rapporti per uso amministrativo o di revisione contabile

Federation Services

- Rappresentano i servizi di federazione verso Identity Provider Esterni, garantendo la piena compatibilità con i più diffusi sistemi di autenticazioni federati (SPID, eIDAS, CNS, etc.).

Industry Standard - PaaS Big Data

Il servizio Industry Standard «PaaS Big Data» è un servizio cloud che fornisce gli strumenti necessari agli sviluppatori, data scientist e analisti per la raccolta, l'archiviazione, l'elaborazione e l'analisi di grandi set di dati. Utilizzata per la gestione di grandi volumi e varietà di dati, la piattaforma è in grado di eseguire analisi avanzate e ottenere informazioni significative attraverso l'elaborazione distribuita e la creazione di pipeline di dati. Tale soluzione permette anche l'integrazione con schedulatori di risorse esterne (YARN, Kubernetes), ed è progettata per essere utilizzata con una vasta gamma di linguaggi.

Principali moduli funzionali disponibili all'interno del servizio Big Data

Data Lake

- Questa soluzione PaaS fornisce una piattaforma pronta all'uso che dispone di tutte le funzionalità necessarie a sviluppatori, Data Scientist e analisti per archiviare facilmente dati di tutte le dimensioni e formati

Batch Batch/Real time Processing

- Questa soluzione PaaS fornisce una piattaforma pronta all'uso per sviluppare processi batch e in streaming basati su un motore di esecuzione in Memory e basato su scalabilità orizzontale e parallela

Event Message

- Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per sviluppare applicazioni e pipeline di dati in real time, inoltre deve fungere da Message Broker fornendo funzionalità di tipo Publish e Subscribe

Data Governance

- Questa soluzione PaaS fornisce una piattaforma pronta all'uso che mette a disposizione un unico punto di riferimento sicuro e centralizzato per il controllo dei dati
- Sfruttando strumenti di "search and discovery" e i connettori per estrarre metadati da qualsiasi sorgente di dati, permette di semplificare la protezione dei dati, l'esecuzione delle analisi e la gestione delle pipeline, oltre ad accelerare i processi ETL

Industry Standard - PaaS AI

Il servizio Industry Standard «PaaS AI» è un servizio cloud che mette a disposizione un set di algoritmi pre-addestrati di intelligenza artificiale (basato su opensource), da utilizzare in diversi contesti applicativi (es: ricerca similarità semantica nel testo, analisi audio e analisi video). Con PaaS AI, gli sviluppatori possono accedere a un insieme di strumenti, librerie e servizi predefiniti che consentono loro di incorporare funzionalità di intelligenza artificiale nelle proprie applicazioni.

Principali moduli funzionali disponibili all'interno del servizio AI

AI Platform

- Viene resa disponibile una piattaforma pronta all'uso per costruire modelli di ML/DL facilitando l'accesso al dato mettendo a disposizione un ambiente collaborativo a cui partecipano sia esperti di contesto che Data Scientist

Semantic Knowledge Search

- Viene fornita una piattaforma pronta all'uso in grado di rendere facilmente accessibili le informazioni contenute all'interno del patrimonio informativo (documenti, immagini, video) utilizzando un motore di ricerca semantico in grado di interpretare richieste in linguaggio naturale

Text Analytics/NLP

- Viene resa disponibile una piattaforma pronta all'uso in grado di estrarre informazioni da testo non strutturato

Audio Analytics

- Viene fornita una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti audio

Video Analytics

- Piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti video; tale soluzione consente di analizzare grandi volumi di video

Industry Standard - CaaS

Il servizio Industry Standard «CaaS» è un servizio cloud che mette a disposizione una piattaforma per l'erogazione dei Container basata su Kubernetes, per abilitare e semplificare la trasformazione delle applicazioni della PA in logica cloud-native e microservizi. Le opzioni disponibili, che la PA può scegliere in base alle proprie esigenze, sono "CaaS Licensed" basato su VMware Tanzu e "CaaS Opensource" basato su Red Hat OpenShift Container Platform. PSN avrà la responsabilità della gestione infrastrutturale e di sicurezza di tutto lo stack tecnologico a supporto.

VMware (Tanzu)

VMware Tanzu è una suite di prodotti e servizi progettati per semplificare l'adozione e la gestione delle moderne applicazioni containerizzate e basate su microservizi. È progettato per consentire alle aziende di sviluppare, eseguire e gestire applicazioni in modo più agile ed efficiente utilizzando le tecnologie dei container.

VMware Tanzu licenced, integra e sfrutta in modo nativo tutti i servizi IaaS PSN.

APPROFONDIMENTI



Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform è la più utilizzata piattaforma opensource per lo sviluppo, deployment e gestione di applicazioni containerizzate basata su Kubernetes in grado quindi di accelerare migrazioni ed eventuali modelli ibridi verso PSN.

Red Hat OpenShift Container Platform garantisce il supporto di tipo enterprise integrato con i servizi PSN.

APPROFONDIMENTI

Versione CaaS Licensed (VMware TANZU) (1/2)

Il servizio Industry Standard «CaaS Licensed Tanzu» è un servizio cloud CaaS basato sullo stack tecnologico IaaS VMware, con l'integrazione nativa di ulteriori due componenti:

- Tanzu Kubernetes Grid
- Cloud Director Container Service Extension (o CSE)

VMware Tanzu Kubernetes Grid (TKG) è una soluzione CaaS di VMware per ambienti Enterprise, che facilita la creazione e la successiva gestione dell'intero ciclo di vita (LCM) dei cluster Kubernetes "upstream" e "fully conformant" (come da specifiche CNCF). Questo conferisce a TKG, le caratteristiche di sostenibilità, conformità ed affidabilità completamente integrata con la piattaforma IaaS sottostante, che ne fanno una soluzione adatta all'impiego in un contesto Enterprise e critico come quello offerto da PSN.

Caratteristiche principali di CaaS Licensed Tanzu:

- Pacchettizzazione Enterprise di soluzioni open source e relativo supporto
- Conforme a Kubernetes open source, con possibilità di scegliere tra diverse versioni di k8s supportate (ultima, ultima-1, ultima-2)
- No lock-in, garantita la portabilità dei container su qualsiasi altro ambiente conforme al progetto Kubernetes
- Estrema facilità d'uso grazie alla completa automazione del lifecycle ed integrazione con la piattaforma infrastrutturale
- Cluster K8s dedicati per il massimo controllo e la massima sicurezza

Versione CaaS Licensed (VMware TANZU) (2/2)

Servizi inclusi

Tutti i servizi già compresi nello **IaaS Shared** ed inoltre:

- Gestione Piattaforma: servizio H24 di secondo e terzo livello per la gestione della piattaforma di containerizzazione e dei relativi cluster Kubernetes;
- Security Operation Center (SOC): Gestione della Sicurezza dell'infrastruttura sottostante il servizio fino al runtimes, secondo la matrice di responsabilità definita;
- Console per la gestione del lifecycle dei container (creazione, cancellazione, modifica).



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Object storage, NAS, Block storage; opzione standard o high performance; opzione encryption
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection (backup, golden copy, DR)
- Business continuity (HA)
- Antivirus
- Banda aggiuntiva dedicata

Servizi Professionali Elementi opzionali a listino Progettazioni dedicate

Versione CaaS Opensource (OpenShift) (1/2)

Il servizio Industry Standard «CaaS Open Source» è un servizio cloud che permette alla PA di sviluppare e gestire applicazioni cloud native basata su piattaforma Red Hat OpenShift Container Platform, una potente piattaforma di orchestrazione dei container basata su Kubernetes, sviluppata da Red Hat. Essa offre agli sviluppatori e agli amministratori un ambiente completo per creare, distribuire e gestire applicazioni containerizzate in modo sicuro e scalabile.

Vantaggi di Red Hat OpenShift Container Platform:

- Ambiente ibrido e multi-cloud, progettato per funzionare su diverse infrastrutture, inclusi ambienti on-premises e cloud pubblici;
- Kubernetes Enterprise-Grade. Essendo basata su Kubernetes, la piattaforma offre tutte le funzionalità di Kubernetes, arricchite da strumenti e funzioni aggiuntive sviluppati da Red Hat per garantire un'esperienza più fluida e affidabile;
- Automazione e Scalabilità, OpenShift semplifica il processo di deployment e scalabilità delle applicazioni containerizzate;
- Sicurezza Integrata, la piattaforma è progettata per garantire la sicurezza delle applicazioni containerizzate, offrendo funzionalità come la scansione delle immagini dei container, il controllo degli accessi basato sui ruoli (RBAC), e la crittografia dei dati sensibili;
- Marketplace e Operator Hub, OpenShift fornisce un vasto marketplace di applicazioni e servizi, insieme all'Operator Hub che semplifica l'installazione e la gestione di servizi complessi basati su Kubernetes;
- Supporto e Community, Red Hat fornisce un supporto enterprise affidabile per OpenShift, garantendo assistenza tecnica, aggiornamenti e patch per mantenere l'ambiente sempre sicuro e aggiornato.

Versione CaaS Opensource (OpenShift) (2/2)

Servizi inclusi

Tutti i servizi già compresi nello **IaaS Shared** ed inoltre:

- Gestione Piattaforma: servizio H24 di secondo e terzo livello per la gestione della piattaforma di containerizzazione e dei relativi cluster Kubernetes;
- Security Operation Center (SOC): Gestione della Sicurezza dell'infrastruttura sottostante il servizio fino al runtimes, secondo la matrice di responsabilità definita;
- Console per la gestione del lifecycle dei container (creazione, cancellazione, modifica).



Possibili servizi aggiuntivi

- IP pubblici (singolo, multiplo)
- Object storage, NAS, Block storage; opzione standard o high performance; opzione encryption
- Servizi di IT Service Operations/Security Services on-top alla gestione dell'infrastruttura
- Data Protection (backup, golden copy, DR)
- Business continuity (HA)
- Antivirus
- Banda aggiuntiva dedicata

Servizi Professionali | Elementi opzionali a listino | Progettazioni dedicate

Data Protection - Backup e Golden Copy

Il servizio Industry Standard «Data protection - Backup» è un servizio cloud che permette di effettuare in autonomia sia i backup che i restore (modalità self-managed) attraverso un'unica console centralizzata integrata con tutti i servizi di PSN sia Private Cloud che CSP.

Il servizio si applica come opzione aggiuntiva ai servizi Industry Standard ed applicabile per tutti i servizi (sia su cloud privato che su CSP). Il servizio effettua una prima copia locale al datacenter primario e una seconda copia (remote vault) su seconda zona della region primaria (backup) o su region differente (Golden Copy) a garanzia della massima sicurezza di immutabilità e del recovery del dato.

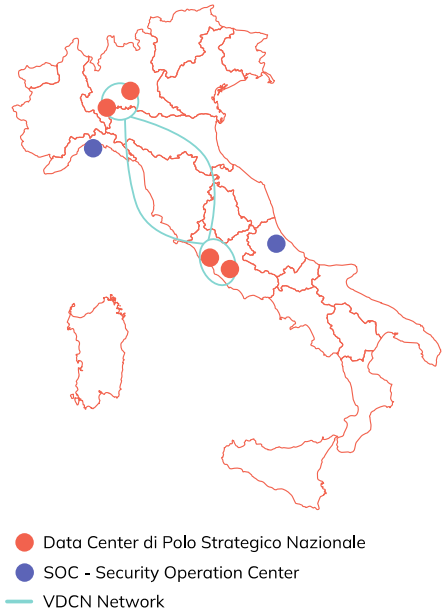
Il Servizio Industry Standard «Data protection - Golden Copy», è un opzione aggiuntiva di sicurezza al servizio di backup che prevede un'ulteriore funzionalità avanzata che analizza i backup allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione. Questa modalità garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many), all'interno di uno storage distinto di backup (privo di ogni accesso fisico e logico) e la replica in Region diversa dalla produzione su canale cifrato.

Data Protection - Opzione DR

Il servizio «Data Protection - Opzione DR» è un servizio opzionale legato ai servizi cloud Industry Standard, che consente il ripristino dell'infrastruttura delle PA o su stessa Region (diversa Availability Zone) o su Region differente, a seguito di un evento disastroso. Il servizio consente alle PA di gestire in autonomia la configurazione, le policy e i relativi test, in modalità integrata con i servizi Industry Standard, dei propri servizi infrastrutturali PSN in linea agli RPO e RTO sotto definiti.

La configurazione infrastrutturale è quindi completamente ridondata grazie alla suddivisione di ognuna delle due Region (Nord e Sud, distanti tra loro circa 500 chilometri in linea d'aria) in *dual-AZ* (Availability Zone), cioè una coppia di Data Center in configurazione di business continuity, distanti tra loro diverse decine di chilometri in linea d'aria.

La ripartenza dei workload protetti dalla soluzione di DR scelta, fornisce alla PA la piena autonomia nella gestione del riavvio di ogni singola applicazione, secondo i piani di DR definiti dalla PA. Grazie a queste predisposizioni e configurazioni è possibile ottenere, in base alle caratteristiche del servizio DR prescelto (intra/inter region), la conformità a valori di RTO (Recovery Time Objective) e di RPO (Recovery Point Objective) per la relativa infrastruttura, fino ai valori più stringenti disponibili e riportati in figura.



«Opzione DR» - Opzioni	RTO	RPO
Opzione DR su stessa Region	10 minuti	30 secondi
Opzione DR su Region differenti	25 minuti	10 minuti

Polo Strategico Nazionale



5.

Servizi Cloud con Cloud Service Provider

Public Cloud PSN Managed

Il servizio «Public Cloud PSN Managed» è un servizio cloud gestito da personale PSN ed è basato sulla tecnologia «Oracle Alloy», con le rispettive region situate in Italia e all'interno dei Data center PSN.

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 separazione logica e/o fisica, sia nella gestione operativa del servizio che nel rilascio e controllo sulle procedure di rilascio del software.

Vantaggi e caratteristiche del servizio:

- **Gestione dei servizi**: effettuata da personale PSN certificato sulle specifiche tecnologie messe a disposizione da Oracle;
- **Gestione dei controlli**: effettuata da personale PSN volta ad analizzare l'eventuale rilascio di funzionalità e/o pacchetti software prima che questi vengano applicati ai servizi PSN. Ciò include audit del codice, l'accesso alla telemetria di sicurezza e strumenti per applicare e monitorare l'implementazione dei controlli;
- **Audit sulle modifiche**: classi di accesso amministrativo ai dati, implementazioni di sistemi critici, deploy e modifiche del codice, modifiche operative che prevedono un'approvazione esplicita da parte di PSN per il completamento;
- **Accesso da parte dei CSP**: per attività di incident/escalation verificato, controllato e approvato solo in casi eccezionali con la possibilità di tracciare tutte le operazioni eventualmente eseguite.

Hybrid Cloud on PSN Site

Il servizio cloud «Hybrid Cloud on PSN Site» di PSN mette a disposizione servizi basati su Cloud Service Provider Microsoft Azure che prevedono la possibilità di utilizzare data center e infrastrutture proprie di PSN per erogare servizi IaaS e PaaS Azure la cui gestione è demandata a PSN.

Tali infrastrutture registrate nelle subscription dei clienti, diventeranno il «deployment target», e saranno utilizzabili attraverso il control plane di Microsoft Azure (Portale, Powershell, CLI, Rest API, ...) per mezzo del servizio Microsoft Azure Arc.

Vantaggi e caratteristiche del servizio:

- Infrastrutture implementate su **paradigma SDDC** certificato per Microsoft Azure con a disposizione **servizi di virtualizzazione** delle componenti di Compute, di Storage e di Network;
- **Infrastruttura dedicata** per singola PA con possibilità di variare tra 2 e 16 nodi computazionali, basati su **server validati** per ottimizzare le performance e la capacity;
- **Disponibilità di servizi Cloud Native di tipo PaaS:** *Orchestrazione di container-Kubernetes; DB-as-a-service - SQL & PostgreSQL; Web App Services - FaaS, Logic App; Machine learning & AI Service;*
- **Gestione del ciclo di vita** dei servizi in modalità **«self-managed»** da parte delle PA grazie al portale Microsoft Azure (come previsto per il servizio Secure Public Cloud);
- Possibilità di definire **un set di policy di sicurezza e di monitoraggio**, che verranno propagate e applicate a tutti i workload delle PA che avranno sottoscritto il servizio.

Secure Public Cloud

Il Servizio «Secure Public Cloud» è un servizio cloud di PSN che si basa su servizi pubblici degli *Hyperscaler Microsoft Azure*, Google Cloud, Oracle e AWS, con Region in territorio italiano. Il controllo e la protezione del dato sono garantiti attraverso specifiche misure di sicurezza e gestione.

PSN realizza gli aspetti di sicurezza e sovranità integrati con i servizi standard del Public Cloud Provider per consentire la gestione dei dati critici.

La **Sicurezza** è garantita da diversi aspetti quali:

- **Gestione delle chiavi di cifratura**: tutti i workload della PA sono cifrati con chiavi (BYOK) di proprietà della PA, gestite da PSN e localizzate all'interno dei centri servizi di PSN;
- **Posture di sicurezza** predefinita, testata e implementata per ogni PA in linea alle principali best practice e framework di riferimento;
- **Gestione del Networking**: tutto il traffico viene monitorato attraverso un'architettura Hub & Spoke che consente di controllare la sicurezza tramite firewall, WAF, SIEM.



La **Sovranità** è garantita da diversi aspetti quali:

- **Policy**: tutti i workload vengono eseguiti solo in datacenter italiani del Public Cloud selezionato. Sono resi disponibili solo servizi che hanno la possibilità di essere securizzati con sistemi di gestione esterni delle chiavi;
- **Copia dei dati su infrastruttura PSN**: possibilità di eseguire un backup in DC PSN, oltre quelli dei CSP per garantire la conservazione del dato su infrastruttura PSN

Polo Strategico Nazionale

6.

Servizi Professionali



Security Services & Compliance

PSN renderà disponibili alle Amministrazioni servizi professionali di sicurezza con l'obiettivo principale di supportare le attività di migrazione e verifica.

Migrazione

Il supporto alla migrazione dei workload e delle applicazioni/database delle Amministrazioni prevedono all'interno della progettazione anche specifici ed ulteriori requisiti e controlli di sicurezza, come ad esempio:

- Supporto all'allineamento della strategia di sicurezza alla strategia di migrazione;
- Assessment delle minacce e delle vulnerabilità del AS-IS;
- Redazione del documento di gap analysis dei controlli di sicurezza in ottica di architettura target (TO-BE);
- Supporto all'implementazione dei controlli e delle policy di sicurezza;
- Supporto all'analisi del rischio e alle verifiche di conformità;
- attività di Audit/Pre-audit.



Verifica

Attività di validazione e verifica di sicurezza dei workload migrati in termini di analisi di vulnerabilità come ad esempio:

- Vulnerability Assessment per la rilevazione delle vulnerabilità infrastrutturali, in caso di servizi di housing, hosting e IaaS;
- Static Application Security Testing per i test sul codice sorgente delle applicazioni;
- Dynamic Application Security Testing per i test sulle applicazioni in esecuzione;
- Penetration test applicativo;
- Monitoraggio continuo della sicurezza.

Le due tipologie di servizio sono complementari e permettono di analizzare e indicare eventuale «remediation» applicativa per aumentare ulteriormente il livello di sicurezza dell'infrastruttura in relazione alla specificità delle applicazioni/dati oggetto di migrazione.

IT Infrastructure - Service Operations

I servizi professionali di «IT Infrastructure - Service Operations» garantiscono un livello avanzato ed ulteriore di gestione delle infrastrutture specifiche della singola PA, oltre ai servizi già previsti riguardanti le componenti fisiche e le piattaforme di virtualizzazione. Tali servizi possono anche supportare la PA nell'eventuale gestione delle componenti middleware e/o applicative che sono state oggetto di re-platforming o re-architect.

PSN potrà prendere in carico, previa valutazione, attività come ad esempio: monitoraggio, infrastructure optimization, capacity management, operation management, compliance management, vulnerability & remediation. Inoltre, tramite la Cloud Management Platform (CMP), PSN potrà anche gestire il provisioning e l'orchestrazione di risorse in ambiente multicloud, nonché l'inventory e il Configuration Management, per conto della PA.

Infine, sui sistemi operativi Microsoft e Linux e sugli ambienti middleware, a PSN può essere richiesto il supporto per il System Management, ovvero la gestione ordinaria e straordinaria dei Server fisici o virtuali, dei container e dei Sistemi Operativi, come ad esempio: creazione/gestione delle utenze e degli accessi ai sistemi, controllo del corretto funzionamento del Sistema Operativo, gestione dei log di sistema e verifica delle eventuali irregolarità, gestione dei files di configurazione dei sistemi, problem management di 2° livello, restore in caso di failure di sistema (dai dati di backup), applicazione delle patch/fix, ecc.

Per tali servizi verrà proposto un team composto da un mix di profili professionali specialistici, in base all'ambiente della PA ed ai requisiti specifici della stessa.

Business & Culture Enablement

All'interno del proprio portfolio, PSN mette a disposizione delle PA servizi professionali denominati «Business & Culture Enablement (BCE)», per erogare attività di Change Management, Formazione e Supporto Specialistico. Tali servizi lavorando in sinergia tra loro, abilitano quella cultura organizzativa necessaria alla trasformazione digitale della PA.

Punti nodali di questa trasformazione sono:

Change Management, un servizio di consulenza dedicato alla co-progettazione con le Amministrazioni delle soluzioni organizzative per l'esecuzione del processo di digital trasformation, con particolare attenzione a:

- Modello organizzativo;
- Competenze e modello manageriale;
- Tool collaborativi;
- Employee experience;
- Modello di innovazione.

Modello Formativo, per l'erogazione di un servizio di formazione in modalità e-Learning, attraverso la predisposizione di un'apposita piattaforma e di un'offerta formativa di corsi online di **base** e **personalizzati**, secondo le specifiche esigenze dell'Amministrazione.

Supporto Specialistico, un portafoglio di servizi di consulenza a supporto dell'evoluzione organizzativa in ambito cloud delle PA, suddiviso in 4 ambiti:

- Organizzazione, processi e strumenti;
- Governance programmi e progetti;
- Digital & Cloud Strategy;
- Supporto e-Learning.

Polo Strategico Nazionale

7.

Altri servizi



Connettività

Il servizio «Connettività» consente l'interconnessione tra i DC della specifica PA (di proprietà e non) e i DC di PSN per permettere di ottimizzare le attività di migrazione delle applicazioni/infrastrutture selezionate.

Tale servizio consiste nella fornitura di una connettività dedicata a partire da 1 Gbps su protocollo gigabit ethernet con terminazione nel data center di erogazione dei servizi di PSN.

In caso di connettività richiesta superiore a 1 Gbps, sono previste le bande a 2 Gbps, 5 Gbps e 10 Gbps; per queste bande, per le quali sarà necessaria una proposizione a progetto, l'accesso fisico è realizzato su Lambda Wave (fibra ottica DWDM).

Vantaggi:

- segregazione e riservatezza del traffico di ciascuna VPN paragonabile a quella offerta dalle reti ATM;
- trattamento differenziato del traffico (QoS);
- possibilità di realizzare su ogni singolo accesso di rete fissa una connettività any-to-any tra le sedi dell'Amministrazione, con conseguente ottimizzazione della banda a disposizione del Cliente;
- supporto del piano di indirizzamento IP privato della LAN dell'Amministrazione;
- trasparenza ad un eventuale uso di crittografia, implementata dalle TIR, end-to-end tra le sedi;
- intelligenza IP condivisa tra TIR e router di accesso;
- ampia scalabilità rispetto al numero di sedi per singola VPN;
- gestione della segnalazione IP (routing) tra le sedi demandata al router di accesso.

Multicloud

Il progetto PSN è costruito secondo un modello multicloud e in tal senso già integra ad oggi le soluzioni di tre cloud Provider (Microsoft Azure, Google Cloud e Oracle Cloud) oltre che la soluzione di Industry Standard.

L'offerta «Multicloud» permette di integrare eventuali altri cloud provider in uso da parte della PA (simili o diversi da quelli PSN), all'interno delle piattaforme di gestione offerte da PSN (Console e CMP), come soluzione completa di architetture Hybrid & Multicloud e come interfaccia unica verso il cliente, indipendentemente dal cloud provider di riferimento.

La Console (C) resa disponibile a tutte le Amministrazioni che contrattualizzeranno i servizi proposti da PSN è applicabile anche in un contesto multicloud (cloud PSN e cloud PA) e si integra con le funzionalità delle Cloud Management Platform (CMP), costituendo così un unico punto di gestione per i servizi standard erogati da PSN. Attraverso servizi professionali (opzionali) è poi possibile estendere le capabilities standard con funzionalità aggiuntive e personalizzate.

Le Amministrazioni hanno modo di accedere alla Console attraverso una autenticazione integrata con il Portale della Fornitura e avere una vista completa di tutti i servizi che hanno contrattualizzato, dei relativi consumi e risorse; inoltre possono accedere alle configurazioni tecniche di dettaglio accedendo alla console tecnica dello specifico servizio.

Possono essere inoltre disponibili funzionalità aggiuntive (tramite sviluppi ad-hoc), ad esempio per workflow personalizzati, capacity planning avanzato (es. con scenari «what-if»), o in ambito security multicloud.

Con la soluzione multicloud è anche prevista la possibilità di accedere alle stesse funzionalità disponibili in console attraverso API, per permettere sia l'utilizzo di framework IaC sia integrazione nativa con eventuali piattaforme della specifica PA.

Antivirus

Il servizio «Antivirus» consiste nella fornitura alle Amministrazioni di un servizio Fully Managed EDR/Antivirus basato su tecnologia leader di mercato per proteggere in modo specifico gli ambienti *Workload* e semplificare la protezione di ambienti virtuali, fisici, in cloud ed infrastrutture *container-based* create sui medesimi.

Tale soluzione mette a disposizione servizi next-gen AV, EDR e MDR e garantisce le seguenti funzionalità:

- Network Protection: per limitare accesso su traffico HTTPS e RDP e/o controllo dei contenuti di navigazione su categorie URL;
- Network Attack Defense: che permette di proteggersi rispetto tecniche specifiche di attacco;
- EDR;
- Data Loss Prevention.

Servizi inclusi:

- **Tenant dedicato,** compresa la fornitura delle necessarie subscription per gli agenti da installare sui workload delle amministrazioni;
- **Supporto** alle procedure di installazione e configurazione degli agent sui singoli workload delle amministrazioni;
- **Supporto** al processo di **onboarding;**
- **Gestione centralizzata dell'antivirus**, garantendo tutte le azioni di verifica, configurazione e definizione delle policy ed enforcement;
- **Segnalazione** alle Amministrazioni sullo specifico workload, su cui siano state rilevate problematiche di funzionamento dell'agent;
- **Segnalazione** alle Amministrazioni sugli incidenti di sicurezza rilevati;
- **Supporto remoto** alle Amministrazioni per risoluzione di problemi relativi alla componente Antivirus (agente);
- **Reporting** mensile dello stato di sicurezza dei workload e degli eventi di sicurezza rilevati.

Sistemi Operativi

In aggiunta ai servizi Core IaaS/Hosting PSN (PSN standard/CSP based) è prevista la possibilità di utilizzare sistemi operativi Licensed (Windows/RHEL) come da convenzione e riportati a listino (sistemi operativi).

Sono disponibili le ultime due versioni sia per Windows che per Linux. Inoltre per la parte Linux Red Hat voci specifiche per singola VM o Bare Metal:

- Linux Red Hat per singola VM;
- Linux Red Hat per Bare Metal (2 Socket);
- Windows Server STD CORE (2 core).

Ampliamento del listino

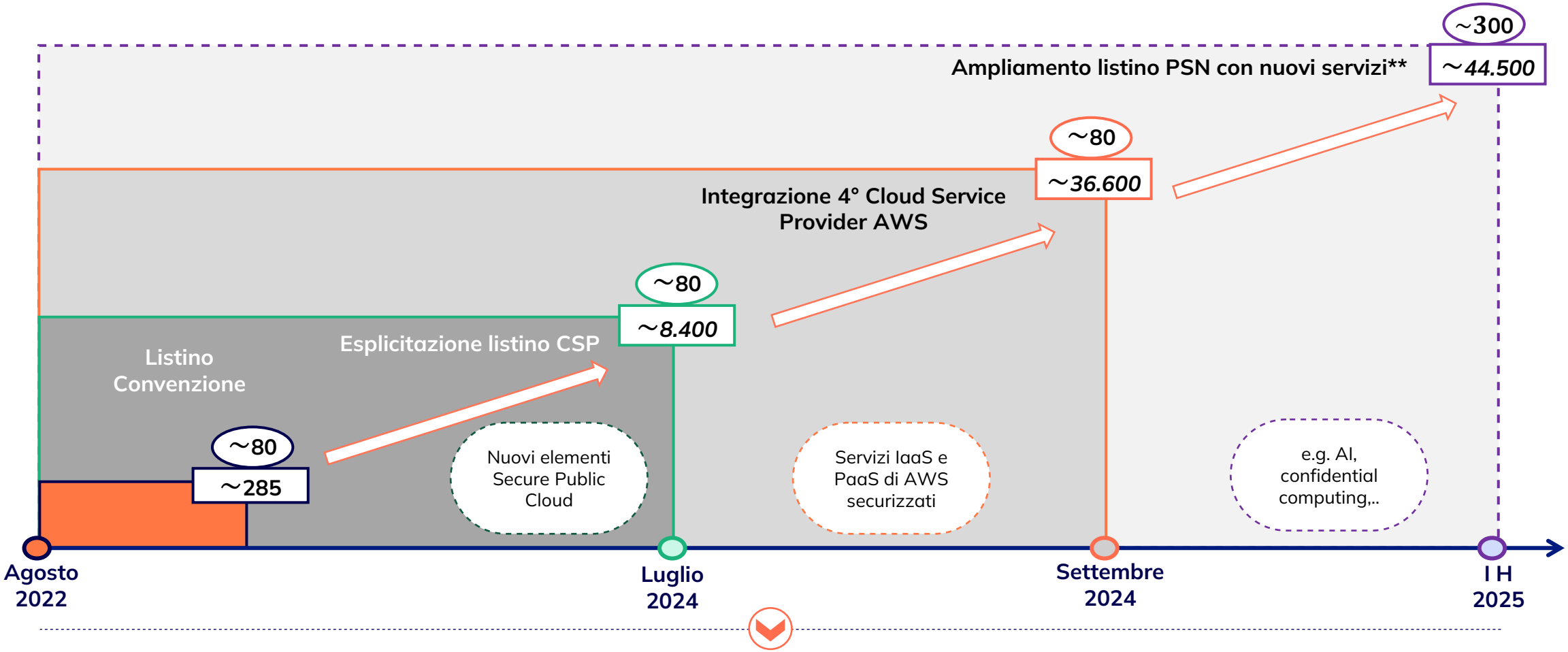
Ampliamento del listino di offerta prodotti, pubblicato nella seconda metà del **2025.**

I servizi aggiunti a listino rientrano nelle seguenti categorie di offerta, di cui vengono forniti maggiori dettagliati nei capitoli successivi:

1. Secure Public Cloud GCP e Azure
2. Public Cloud PSN managed - Oracle
3. Industry standard
4. Supporto Premium

Ampliato il portafoglio di offerta PSN, anche mediante l'introduzione di nuovi servizi

XX # Servizi CSP
XX # Servizi Industry Standard



Offering di PSN ancora più ampio grazie all'introduzione di oltre 44 mila nuovi elementi a listino, sia su industry standard (4x) che CSP (160x)

Polo Strategico Nazionale

Ampliamento listino Secure Public Cloud GCP e Azure

Verranno successiva-mente **esplicitati** i servizi **Atlas MongoDB** e **Database Oracle** per SPC

	# SKU	Descrizione
	**2.477** *Totale 4.486 SKU*	▪ Integrati i servizi **GCP con i servizi IaaS e PaaS rilasciati negli ultimi 2 anni** e inoltre sono state integrate le **nuove famiglie di servizio**: - **AI** - **API** - **SecOps** - **Support**
	**2.210** *Totale 8.429 SKU*	▪ Integrati i servizi Azure con i **servizi IaaS e PaaS rilasciati negli ultimi 2 anni** (incluso il rilascio della Region di Milano) ▪ Introdotti i servizi di **Cognitive services** (particolarmente interessanti sono i servizi di Azure OpenAI)
	**2.981** *Totale 2.981 SKU*	▪ La soluzione **Confidential Public Cloud IaaS** è progettata per fornire **servizi cloud pubblici con un alto livello di sicurezza e sovranità digitale**. Questa soluzione include strumenti di gestione delle chiavi di crittografia, governance e sicurezza per garantire che i dati siano protetti in ogni fase del loro utilizzo. ▪ La piattaforma offre servizi IaaS all'interno dei datacenter dell'hyperscaler garantendo la **protezione delle informazioni basate su confidential computing, OS immutabili e chiavi di crittografia.**

Verranno successiva-mente **esplicitati** i servizi **Atlas MongoDB** e **Database Oracle** per SPC

1.Servizi ampliati Secure Public Cloud GCP

Relativamente ai servizi SPC di Google Cloud Platform, l'integrazione dell'offerta PSN riflette 4 principali evoluzioni tecnologiche occorse:

- **Evoluzione tecnologica** dei prodotti presenti nel catalogo dell'hyperscaler nella **region di Milano** (europe-west8);
- Rilascio e nuova disponibilità di una **seconda Region ubicata a Torino** (europe-west12);
- Introduzione di **nuovi servizi** di **supporto** erogati direttamente dall'Hyperscaler;
- **Esplicitazione della voce** di listino "**Sovereign Controls** ": tramite la configurazione "Sovereign Controls " è possibile impostare delle **policy all'interno di GCP per definire / restringere la localizzazione e memorizzazione dei dati**, la **crittografia** e avere **accesso ai log di sistema** che tracciano il consumo delle chiavi crittografiche (Key Access Justifications – KAJ),

L'integrazione delle nuove SKU nel servizio **Secure Public Cloud GCP** introduce 4 nuove aree strategiche, abilitate dall'evoluzione tecnologica:

- **AI** : Servizi PaaS per sviluppo e deployment di applicazioni **AI/GenAI**
- **API**: Strumenti **abilitanti per la migrazione** di applicazioni modernizzate, fondamentali per l'esposizione di servizi via **API Gateway**
- **SecOps:** Componenti di **sicurezza operativa integrata** (Security Operations) che garantiscono la protezione dei workload dopo la migrazione
- **Support**: Servizi di **monitoraggio, controllo e mantenimento operativo**

Oltre alle SKU GCP recentemente rese disponibili dall'Hyperscaler verranno successivamente resi disponibili i servizi:

- **Database MongoDB per SPC**
- **Database Oracle per SPC**

1. Servizi ampliati Secure Public Cloud Azure

Novità	Descrizione
Nuovi servizi IaaS e PaaS	▪ Integrata l'offerta con servizi **IaaS e PaaS** rilasciati da Azure nel **corso degli ultimi 2 anni**, anche in considerazione della localizzazione dei servizi nella nuova Region di Milano (avvenuta durante l'ultimo trimestre 2023)
Artificial Intelligence	▪ Prevista l'integrazione di diversi servizi di **AI powered by Azure** ▪ Particolarmente interessanti sono i servizi di **OpenAI**: - È un servizio di Microsoft Azure che mette a disposizione delle aziende i **modelli di intelligenza artificiale generativa di OpenAI** (come ChatGPT, GPT-4, Codex, DALL·E, ecc.) all'interno del cloud Azure. - Questi modelli possono: - **comprendere testi** (es. assistenti virtuali, chatbot, riassunti automatici) - **generare contenuti** (testi, immagini, codice) - **automatizzare** risposte, supporto clienti, documentazione - potenziare **analisi e ricerca** semantica nei dati aziendali
Application platform	▪ **Azure Logic Apps** è un servizio di **integrazione e automazione no-code/low-code** offerto da Microsoft Azure. Serve per **creare flussi di lavoro automatizzati** che **collegano app, dati, sistemi e servizi**, senza scrivere codice complesso
Premium Support	▪ Servizi di assistenza premium da parte dell'hyperscaler Microsoft

1. Esplicitazione futura Mongo DB e Oracle su SPC

Mongo DB Atlas

- **Cluster Automation**:
  - **Provisioning automatico** di **server e software MongoDB** (Atlas crea i server virtuali e installa il software MongoDB)
  - **Patch e aggiornamenti** automatici
  - Supporta la **Scalabilità automatica** (verticale e orizzontale) di storage e risorse di calcolo
- **Alta disponibilità**:
  - Replica set distribuiti su più **Availability Zones** dei CSP
  - **Backup continui e ripristini point-in-time**
- **Sharding & Replica**: gestione efficiente di grandi volumi di dati
- **Monitoring & Ottimizzazione**: strumenti avanzati per analisi delle performance e suggerimenti di tuning
- **Sicurezza avanzata**: Integrazione con **HSM PSN**
  - Dati residenti nel Secure Public Cloud
  - Chiavi custodite nelle regioni PSN per maggiore sicurezza e compliance

Oracle DB on SPC

- **Supporto Oracle Nativo**:
  - **Oracle Autonomous Database**: gestione automatica del ciclo di vita
  - **Oracle Exadata**: alte prestazioni per workload critici
  - **Oracle RAC**: alta disponibilità e bilanciamento del carico
  - **Servizi PaaS Oracle** per lo sviluppo e la gestione applicativa
- **Prestazioni e scalabilità**:
  - Risorse di calcolo e storage scalabili
  - Ottimizzazione automatica secondo best practice Oracle
- **Backup & recovery**: gestione tramite **Oracle RMAN**
- **Migrazione semplificata**: tramite strumenti Oracle nativi (es. Active Data Guard, GoldenGate)
- **Sicurezza avanzata**: Integrazione con **HSM PSN**
  - Dati nel cloud pubblico
  - Chiavi gestite in sicurezza nel perimetro PSN

1. Servizi ampliati Secure Public Cloud Azure Confidential

La soluzione è progettata per offrire un livello completo di protezione e controllo, ancora più elevato di protezione e controllo del dato, estendendo le garanzie di protezione anche alla fase di elaborazione, oltre a quelli standard previsti (crittografia dei dati in trasmissione e salvataggio).

Questa piattaforma si basa esclusivamente su componenti che **non necessitano la decriptazione dei dati per l'elaborazione**, grazie all'utilizzo esclusivo di:

- Risorse di calcolo **stateless** (ovvero che **non archiviano dati**) oppure
- Risorse basate su **confidential computing** (che permette **l'elaborazione dei dati cifrati anche in memoria**), come ad esempio:
  - VM Confidential
  - Ledger Confidential
  - Databricks Confidential
  - Kubernetes Confidential

Inoltre:
Le **SKU** disponibili in SPC Confidential Azure rappresentano una **sotto selezione del listino generale SPC Azure**, includendo solo quelle compatibili con i requisiti di sicurezza e riservatezza previsti.

A parità di SKU (es. le stesse VM confidential), il **servizio erogato alla PA è differente** tra le due offerte (SPC Azure e SPC Confidential Azure), in quanto nella versione Confidential l'intera configurazione dell'ambiente cloud è strutturata per garantire il massimo isolamento e protezione dei dati.

Questa architettura garantisce:

- L'integrità dei dati anche durante l'elaborazione
- Un controllo completo da parte del PSN, senza mai cedere la gestione delle chiavi crittografiche al CSP
- Una separazione netta e verificabile tra i dati della PA e l'infrastruttura del cloud provider

2. Public Cloud PSN managed - Oracle

- Integrati 232 item relativi al servizio **Oracle Alloy**
- Tali elementi sono veicolati da PSN tramite il servizio **Public Cloud PSN managed** che prevede l'erogazione su region italiane, operato e controllato da personale di PSN, con separazione logico-fisica dalla parte pubblica del CSP

Core Infrastructure

Integrate con voci di listino relative a **infrastruttura core** (OCPU, RAM, …) oltre a nuovi servizi OCI, processori **5° gen AMD** e servizio Oracle Cloud Vmware Solutions (**OCVS**)

Data Management

Permette di scegliere tra diverse versioni e configurazioni di servizi **DBMS** basati su tecnologia Oracle (i.e., ExaData, Base Database Service, Autonomous Database, …)

AI e Machine Learning

Una suite completa di servizi avanzati basati su **IA e ML** (Data labeling, Speech, Image analysis, OCR, …)

Security

Previsti diversi servizi di sicurezza (App Firewall, Identity mgmt, Monitoring …)

Developer services

Strumenti avanzati progettati per migliorare lo **sviluppo delle applicazioni**, la **gestione dei server** e **l'integrazione delle API** (e.g. Oracle Visual Builder)

Application

Software evoluti che permettono alle PA di eseguire applicazioni in **modo serverless**

DR

L'implementazione di **Oracle Alloy** permette di utilizzare attualmente le funzionalità di **ridondanza di un Availability Domain**. Si **creerà una seconda region Alloy nella region Nord**, con l'obiettivo di replicare i medesimi livelli di disaster recovery presenti nell'implementazione pubblica di OCI

2. Servizi ampliati Public Cloud PSN managed (1/4)

Core Infrastructure

Include i principali servizi infrastrutturali a supporto delle PA per l'esecuzione di carichi di lavoro in cloud con alte prestazioni e flessibilità:

- **Compute**: VM, Bare Metal, GPU (A100, A10, L40S), Confidential computing
- **VMware Solution**: migrazione e gestione nativa di ambienti Vmware
- **Storage**: Block, Object, File (ZFS)
- **Networking & FastConnect**: connettività avanzata e sicura
- **Container & Serverless**: supporto a Kubernetes e architetture moderne

Grazie ai nuovi hardware (X11) e alle CPU AMD EPYC E5, il servizio offre prestazioni fino a 2x superiori. La soluzione consente una migrazione fluida, mantenendo strumenti e competenze esistenti, e garantisce scalabilità, sicurezza e performance avanzate

Data management

Soluzioni avanzate per la gestione scalabile dei dati, pensate per soddisfare le esigenze applicative e prestazionali delle PA:

- **Database Oracle**: Exadata, Base Database Service, Autonomous Database
- **Motori specializzati**: Oracle HeatWave (elaborazione in-memory), NoSQL, Hadoop (gestione dati distribuiti)
- **Flessibilità**: storage configurabile in base alle reali esigenze, per ottimizzare costi e risorse
- **Tecnologia aggiornata**: supporto ai nuovi processori AMD EPYC per migliori performance

La PA può scegliere l'approccio tecnologico più adatto al proprio scenario, beneficiando di prestazioni elevate, scalabilità e piena integrazione con l'infrastruttura PSN Managed.

2. Servizi ampliati Public Cloud PSN managed (2/4)

AI e machine learning

Suite completa di servizi AI/ML per automatizzare processi, migliorare l'efficienza operativa e valorizzare i dati delle PA:

- **Servizi AI ready-to-use**: chatbot intelligenti, anomaly detection, sentiment analysis, OCR, riconoscimento vocale e visione artificiale
- **Modelli personalizzabili**: training su dati specifici per linguaggio, immagini e documenti
- **Data Labeling & Document Understanding**: etichettatura dati, estrazione di informazioni e proprietà documentali
- **Generative AI**: modelli avanzati (Cohere, Llama2-70) per creare contenuti e automatizzare processi
- **WebCenter Suite**: strumenti integrati per la gestione di contenuti, portali, documenti e siti web aziendali

Tutti i servizi sono **erogati all'interno del perimetro PSN**, accessibili via API, in modalità *As-a-Service* e nel pieno rispetto della **sovranità e sicurezza dei dati**.

Security

Soluzioni avanzate per la protezione, il monitoraggio e la gestione sicura degli ambienti cloud della PA:

- **Firewall**: Application e Enterprise Firewall per traffico web; Network Firewall per protezione multi-livello
- **Identity Management**: gestione utenti e accessi, MFA, supporto per utenti/app esterni, replica multi-region
- **Security Monitoring**: rilevamento minacce, assessment di vulnerabilità, advisory basati su AI
- **Observability**: health check, metriche, log analytics, performance monitoring, alerting e insights operativi
- **Key Management**: gestione sicura e sovrana delle chiavi crittografiche per protezione dei dati
- **Sensitive Data Protection**: identificazione, mascheramento e rimozione automatica di dati sensibili

Tutti i servizi sono progettati per garantire **sicurezza, compliance e sovranità** dei dati nel perimetro PSN, con strumenti *as-a-service* integrabili e centralizzati.

2. Servizi ampliati Public Cloud PSN managed (3/4)

Developer services

Strumenti avanzati per accelerare e semplificare lo sviluppo applicativo nella PA:

- **Visual Builder**: piattaforma low-code per creare rapidamente applicazioni web e interfacce utente intuitive, con supporto all'intero ciclo di vita del software
- **WebLogic Server**: application server per l'esecuzione di applicazioni Java EE, utilizzabile sia in ambienti tradizionali che containerizzati (es. Kubernetes)
- **Oracle APEX**: ambienti e acceleratori per lo sviluppo rapido di applicazioni web dinamiche con approccio low-code

I servizi sono pensati per **ottimizzare tempi di sviluppo, favorire l'adozione di tecnologie moderne** e garantire **scalabilità e integrazione fluida** con l'ecosistema PSN.

Application

Soluzioni per l'esecuzione serverless e l'integrazione applicativa, pensate per la modernizzazione delle PA:

- **Servizi Serverless**
  - Esecuzione di codice senza gestione infrastrutturale
  - Architetture **event-driven** con scalabilità automatica
  - Focus sullo sviluppo della logica di business, senza overhead sistemistico
- **API Integration & Data Flow**
  - Integrazione in tempo reale, batch e streaming tra sistemi eterogenei
  - Soluzioni come **GoldenGate**, **Oracle Integration Cloud**, **Process Automation**
  - Supporto a diversi protocolli e formati, orchestrazione di processi complessi
  - Alimentazione di data lake/warehouse e supporto a decisioni data-driven

Tutti i servizi sono progettati per **scalabilità, sicurezza e interoperabilità**, nel pieno rispetto dei requisiti del PSN.

2. Servizi ampliati Public Cloud PSN managed (4/4)

Disaster Recovery

Architettura progettata per garantire **massima disponibilità e continuità operativa**:

- **Struttura Alloy del PSN**
  - **2 Region Alloy** (Sud attiva, Nord in attivazione entro Q3 2025)
  - **3 Fault Domain per Region** → isolamento fisico e logico
  - **Anti-affinità**: istanze distribuite su hardware diversi
  - **Alta resilienza**: fault domain indipendenti

- **Continuità Operativa e DR**
  - **Protezione da disastri regionali**
  - Attualmente la **gestione dei tenant** è completamente **demandata alla PA** e in **fase progettuale viene definito con un enabler**
  - **104 campionamenti/anno** per verifica operativa

- **Sovranità dei Dati**
  - Tutti i dati residenti nei **Data Center PSN**
  - **Rete esclusiva** tra Region (no internet pubblico)
  - Configurazioni all'interno del perimetro di sicurezza PSN
  - **Cifratura** secondo specifiche ACN per dati critici e strategici

Tutti i servizi PSN Managed Oracle sono attivi e contenuti nella piattaforma Alloy, completamente **inclusa nel perimetro di sicurezza PSN**

3. Industry standard

Housing

Soluzione di spazio delimitato e servizio ALE

Hosting

Integrato con soluzione di WAF (Web application firewall di Fortinet e analoghe)

Compute

IaaS private GPU, CaaS, IaaS private con AMD ecc.

Storage

Soluzioni di Block storage e Object storage

Operating System

Rivendita di nuovi Sistemi Operativi

Networking

Servizi di cloud interconnect (volto a semplificare la migrazione), IP pubblico singolo, DNS

Security

Servizi di NGFW, End point protection, IAM, PAM, key vault ecc.

Database

Estensione dei servizi PaaS DB già esistenti del PSN con la logica di introdurre modelli di deployment multitenant con logiche differenziate non attualmente disponibili (Zonal, HA, DR)

Middleware

Integrazione di servizi «CaaS», «IaaS shared», «PaaS Big Data» prevedendo soluzioni di API platform, APP Runtime, BPM, CMS, DAM, ETL, Event platform, Form platform, Integration Platform, Search engine

Data Protection

Specifiche integrazioni sui servizi di Backup (Backup per PaaS DB, BAAS on premise, Cyber Recovery and Vault) oltre che servizi di DR per PaaS

3. Industry standard

Infra & Ops platform

Integrazione di specifiche piattaforme per la gestione dei servizi (e.g. portali per la gestione self service, soluzioni di monitoraggio ecc.)

Devsecops

Servizi di **Continuous Integration e Continuous Development** di software in modo che siano progettati per **automatizzare e ottimizzare il processo di sviluppo**, garantendo che ogni modifica al codice sia testata e verificata immediatamente

Big data

Definiti servizi per **Business Intelligence, Columnar / Time Series, Data Governance, Data Lakehouse, Data Scientist Platform e GIS TECHNOLOGY**

Collaboration

Soluzione Mattermost (piattaforma di messaggistica e collaborazione open source che offre strumenti sicuri per la comunicazione in team, la condivisione di file e l'integrazione con altre applicazioni, supportando la produttività in ambienti di lavoro distribuiti)

AI

Introdotte soluzioni di **Audio & Convenzioni, GenAI, Image analysis and elaboration, Text analysis and elaboration, Tools** (piattaforme avanzate di AI), **Video analysis.**

VDI

La **Virtual Desktop Infrastructure** permette agli utenti di accedere e gestire **dekstop virtuali** ospitati su server centralizzati

Housing



	Dettagli	Descrizione
Spazio delimitato contiguo (security cage) - STANDARD	▪ Altezza pareti 2,7 t	▪ Servizio che offre alle Pubbliche Amministrazioni uno spazio fisico dedicato e protetto (in gabbia), utile per ospitare apparati legacy non migrabili al cloud. È pensato per **apparati che gestiscono dati critici o strategici**, garantendo isolamento fisico e sicurezza elevata.
Spazio delimitato contiguo (security cage) - PREMIUM	▪ Altezza delle pareti fino al soffitto	▪ Servizio che aggiunge, alla versione Standard, **pareti di sicurezza alte fino al soffitto.**
Servizio ALE (Advanced Live Environment)	▪ 1 Tenant sul sistema ALE comprensivo di 5 licenze client	▪ Piattaforma immersiva che permette di **gestire visivamente i Data Center in 3D.** Consente di navigare virtualmente tra gli apparati, visualizzare l'infrastruttura reale, asset e spazi, e **identificare rapidamente anomalie o discrepanze**. L'accesso avviene tramite un client installato con licenza su PC, tablet windows o notebook.

CaaS + Function as a Service

Il nuovo modello CaaS **integra l'approccio serverless con Function as a Service**, permettendo l'esecuzione di funzioni a evento senza gestione diretta dell'infrastruttura.
Una soluzione ideale per **microservizi e automazioni nella PA.** L'infrastruttura evolve con **ControlPlane dedicato per ogni tenant**, supporto multi-AZ e reti completamente isolate.
Ogni tenant dispone di endpoint e console autonomi, può gestire progetti, operator e aggiornamenti in autonomia, con privilegi in stile ClusterAdmin. Grazie a **Portworx Enterprise**, vengono introdotti **volumi RWX** e soluzioni avanzate di **backup e disaster recovery cross-region** con **Commvault e Portworx-DR**. Una piattaforma moderna, flessibile e sicura, pronta per le esigenze della digitalizzazione pubblica.

CAAS - ADDON

- **AI (4 Vcpu):** risorse dedicate per eseguire applicazioni di intelligenza artificiale all'interno dell'ambiente containerizzato.
- **STORAGE (RWX) (1 Worker Node):** storage condiviso tra più pod con possibilità di lettura/scrittura simultanea, gestito da un nodo dedicato.
- **ADVANCED CLUSTER MANAGEMENT (4 Vcpu):** strumento per il controllo centralizzato di cluster Kubernetes multipli, con funzionalità avanzate di governance e monitoraggio.

CAAS - PRIVATE

- Virtual Control Plane
- Virtual Worker (Small)
- Virtual Worker (Medium
- Virtual Worker (Large)

- Infrastruttura basata su macchine virtuali ospitate su hw dedicated
- ControlPlane gestita dalla PA
- Ogni cliente avrà il proprio Endpoint per le API del cluster e la propria Console dedicata

CAAS – SHARED

- Virtual Worker - Small – Okd
- Virtual Worker – Small
- Virtual Worker – Medium
- Virtual Worker – Large

- Infrastruttura basata su macchine virtuali ospitate su hw shared
- Control Plane gestita dal PSN



Private Confidential: IaaS e Kubernetes

Il servizio **Confidential - IaaS – Private** è progettato per la **gestione dei dati più sensibili**, offrendo un livello di sicurezza e isolamento superiore.

Questo è possibile grazie a:

Risorse Hardware Dedicate: L'ambiente IaaS Private è completamente isolato e le sue risorse non sono mai condivise.

Cifratura Dati in Uso (TEE): Protezione tramite enclave hardware (TEE) che mantiene i dati cifrati non solo a riposo e in transito, ma anche durante l'elaborazione.

Verifica con Remote Attestation: Processo crittografico che fornisce la prova matematica dell'integrità e dell'autenticità dell'ambiente, garantendo che sia sicuro prima di inviare i dati.

Servizi Disponibili:

IaaS Private Confidential

- Pool Small (3 Host)
- Pool Medium (6 Host)
- Pool Large (9 Host)
- Pool X-Large (12 Host)

Canone fisso annuale, su risorse HW dedicate (CPU/RAM/Storage). Ambienti completamente isolati e sicuri.



PaaS - Confidential Kubernetes

Estende le stesse garanzie di sicurezza, cifratura e attestazione al mondo dei container per le applicazioni moderne.

IaaS private con hypervisor



Servizio IaaS basato su **VMware Cloud Foundation**, pensato per la PA, con risorse dedicate e gestione autonoma da parte del cliente.
La piattaforma **include** licenza VCF, server dimensionati per cluster VMware, **backup personalizzabile**, privilegi in stile **Cluster Admin** e supporto a scenari di multi-tenancy e Disaster Recovery.

L'hardware è gestito interamente da PSN.

Infrastruttura fisica + Hypervisor (BYOS)

Piattaforma di virtualizzazione gestibile in autonomia, da licenziare con VCF del cliente.

Infrastruttura fisica + Hypervisor (Licenza Inclusa)

La piattaforma è gestibile in autonomia tramite accesso al vCenter, con diritti amministrativi controllati da PSN.Il cliente non deve gestire l'hardware: è tutto in carico al PSN, su infrastruttura già allocata.

Infrastruttura fisica + Hypervisor + Multi tenant (Licenza Inclusa)

Aggiunge uno strumento di cloud management (VMware Cloud Director) con cui la PA può gestire in autonomia un vero e proprio cloud ai propri clienti ed integrarlo con le proprie soluzioni.

Infrastruttura fisica + Hypervisor (Opz. Iperconvergente):

- **Standard**
- **Advanced**

Si tratta di un servizio IaaS in cui la PA può usufruire di una infrastruttura virtuale con risorse dedicate sulla quale sarà installato l'**hypervisor con tecnologia Iperconvergente**.

SE Standard → include licenza Nutanix Pro

SE Advanced → include licenza Nutanix Ultimate
(licenze adatte per l'erogazione di database)

IaaS GPU



Il servizio IaaS con GPU fornisce **potenza di calcolo specializzata**, ideale per carichi di lavoro grafici e computazionalmente intensivi. Sfruttando la tecnologia di virtualizzazione, le **risorse** di potenti GPU fisiche vengono rese disponibili **on-demand,** consentendo un'allocazione flessibile ed efficiente.

Sono previste due principali modalità di servizio:

Il modello Private GPU assegna le risorse di calcolo in modo totalmente esclusivo, garantendo il massimo livello di performance per le applicazioni più esigenti.

Il modello Shared GPU, invece, offre una frazione della potenza di una GPU.
Questa modalità rappresenta una soluzione versatile e ottimizzata nei costi per un'ampia varietà di applicazioni che richiedono un accesso non esclusivo alla capacità di calcolo.

IAAS - PRIVATE - GPU

- E' un servizio IaaS che rende disponibile alle PA che ne facciano richiesta una GPU in tecnologia Nvidia H100 o similare.
- **1 GPU da 94GB 100% dedicata**

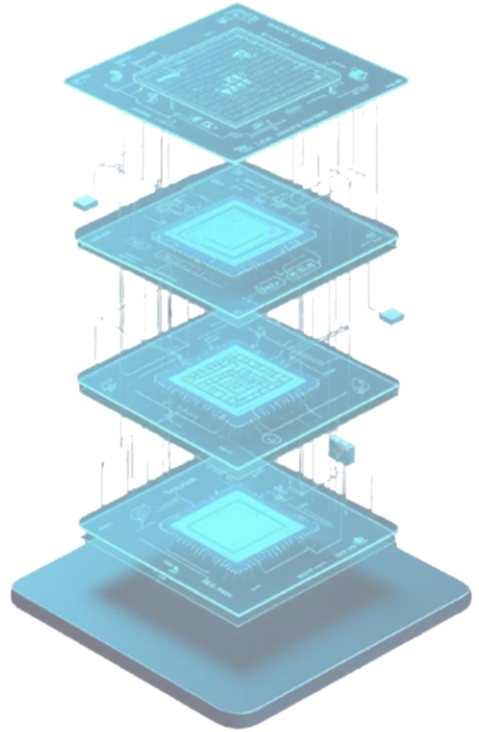
IAAS - SHARED – GPU

- E' un servizio IaaS basato su piattaforma virtualizzata e condivisa che rende disponibile alla PA che ne faccia richiesta una GPU con tecnologia H100 o similare
- **1 GPU da 94GB dedicata al 50%**

IAAS - SHARED – GPU

- E' un servizio IaaS basato su piattaforma virtualizzata e condivisa che rende disponibile alla PA che ne faccia richiesta una GPU con tecnologia Nvidia H100 o similare.
- **1 GPU da 94GB dedicata al 25%**

Altri IaaS private Premium e High Availability (1/2)



Il servizio IaaS – Private Premium offre risorse computazionali dedicate su tecnologia VMware, con processori Intel Sapphire Rapids o AMD EPYC di 4a generazione.
L'offerta prevede due modelli di allocazione:

Reserved: con il 100% delle risorse garantite ad uso esclusivo.
Flex: con il 70% delle risorse garantite e capacità di utilizzo dinamico di quelle non allocate.

L'infrastruttura è progettata per alte prestazioni e supporta configurazioni in **Alta Affidabilità (HA)** per garantire la massima continuità operativa.

POOL LARGE FLEX (4TH GEN INTEL)

Modello di allocazione Flex su tecnologia **Intel Sapphire Rapids** (4ª gen): offre il **70% di risorse garantite** con capacità di utilizzo dinamico della capacità non riservata. L'overcommit delle risorse non è consentito.

POOL LARGE RESERVED (4TH GEN INTEL)

Modello di allocazione **Reserved** su tecnologia **Intel Sapphire Rapids** (4ª gen): offre il **100% di risorse dedicate e garantite**, con possibilità di effettuare overcommit.

POOL LARGE FLEX (4TH GEN AMD)

Modello di allocazione **Flex** su tecnologia **AMD EPYC Genoa** (4ª gen): offre il **70% di risorse garantite** con capacità di utilizzo dinamico della capacità non riservata.L'overcommit delle risorse non è consentito.

POOL LARGE RESERVED (4TH GEN AMD)

Modello di allocazione Reserved su tecnologia **AMD EPYC Genoa** (4ª gen): offre il **100% di risorse dedicate e garantite**, con possibilità di effettuare overcommit.

Altri IaaS private (2/2)

Il servizio IaaS Private si arricchisce di componenti opzionali che permettono di potenziare la sicurezza e garantire la resilienza dei carichi di lavoro.
Gli **Add-on** disponibili consentono di proteggere il traffico di rete con firewall avanzati, prevenire minacce con sistemi di analisi e detection (IDS/IPS, sandboxing, NDR) e attivare meccanismi di Disaster Recovery per il ripristino rapido delle virtual machine in caso di eventi critici.
A complemento, il **Pool IaaS Private SAP** offre risorse di calcolo private, certificate e ottimizzate per eseguire applicazioni SAP o carichi di lavoro ad alto consumo di memoria (memory intensive), come database di grandi dimensioni.

AddOn di sicurezza

vFirewall – *Security Add-on*

- Add-on che rafforza la sicurezza per il traffico est-ovest e nord-sud

vFirewall with Advanced Threat Prevention – *Advanced security Add-on*

- Add-on che introduce strumenti avanzati di security con analisi del traffico e prevenzione (come IDS/IPS, NSX Sandbox e NDR)

Live Recovery Protected VM - *Disaster Recovery Add-on*

- Add-on che aggiunge una soluzione di Disaster Recovery

Pool IaaS Private SAP

Risorse Private (Licenza Inclusa) op. Memory Intensive	**MEDIUM** Pool risorse virtuali private (24vcpu – 768GB)	Servizi di compute privati con infrastruttura large adatta e certificata per eseguire workload ad alto utilizzo di memoria, come ad esempio database. Sono erogati da hardware certificato SAP. Licenze SAP non erogate e non disponibili nel listino PSN.
	LARGE Pool risorse virtuali private (48vcpu – 1536GB)	

IaaS Storage (1/3)

BLOCK STORAGE (1000 GB) - HIGH DENSITY/ HIGH DENSITY HA

Block Storage High Density è un servizio di archiviazione a **elevata capacità**, progettato per rispondere alla crescente domanda delle PA di soluzioni storage economiche e scalabili per la gestione di grandi volumi di dati.

È ideale per applicazioni data intensive, come data warehouse, cluster Hadoop o Spark, dove la **priorità è la capacità di archiviazione piuttosto che le massime prestazioni.**

Il servizio fornisce **blocchi da 1000 GB** con possibilità di configurazione in **High Availability (HA)** su due data center distinti, garantendo resilienza e sicurezza. I dati sono cifrati a livello infrastrutturale con chiave dedicata per ogni tenant, assicurando la protezione completa delle informazioni.

Block Storage (1000 GB) - HIGH DENSITY

Si tratta di **storage a capacità elevata** ottimizzato in base al costo per capacità (prezzo/GB).

Block Storage Encrypted (1000 GB) - HIGH DENSITY

Il servizio è erogato attraverso una piattaforma la cui architettura ne garantisce **l'encryption dei dati a livello infrastrutturale con chiave di PSN**.

Block Storage (1000 GB) - HIGH DENSITY HA

Il servizio è erogato attraverso una piattaforma la cui architettura ne garantisce la **High Availability** mediante l'attivazione di una **replica dei dati** all'interno di una seconda zona della region scelta al momento della creazione del volume.

Block Storage Encrypted (1000 GB) - HIGH DENSITY HA

Il servizio è erogato attraverso una piattaforma la cui architettura ne garantisce:

- **High Availability** mediante l'attivazione di una replica dei dati all'interno di una seconda zona della region scelta al momento della creazione del volume;
- **Encryption** dei dati a livello infrastrutturale con chiave di PSN.

IaaS Storage (2/3)

BLOCK STORAGE (500 GB) – HP/SP PERFORMANCE

Il servizio Block Storage su singola Availability Zone offre **due opzioni** di archiviazione per supportare differenti esigenze applicative della PA.
La modalità **High Performance (HP)** è indicata per applicativi che richiedono alte prestazioni di accesso ai dati, come application server e sistemi critici.
La modalità **Standard Performance (SP)** è pensata per applicazioni meno esigenti in termini di performance, come web application, ambienti non produttivi e carichi di lavoro non mission critical.
Entrambe le soluzioni garantiscono la cifratura dei dati a livello infrastrutturale con chiave dedicata per ogni tenant.
Lo storage è disponibile in blocchi da 500 GB e viene erogato su piattaforma Pure Storage già integrata nell'infrastruttura PSN (Pure FlashArray//C).

Block Storage (500 GB) - HP PERFORMANCE

Il servizio è pensato per consentire la migrazione di applicativi con richieste di storage ad alte prestazioni, come ad esempio **application server.**

Block Storage Encrypted (500 GB) - HP PERFORMANCE

Anche per questo servizio applicativi con richieste di storage ad alte prestazioni, come ad esempio **application server.**
Il servizio è erogato attraverso una **piattaforma** la cui architettura ne **garantisce l'encryption dei dati a livello infrastrutturale con chiave di PSN.**

Block Storage (500 GB) - SP PERFORMANCE

Il servizio è pensato per consentire la migrazione e la creazione di applicativi che non richiedono elevate prestazioni di accesso ai dati, come ad esempio **Web Application, FE, applicativi non mission critical, ambienti non produttivi.**
Il servizio è erogato attraverso una piattaforma la cui architettura ne **garantisce l'encryption dei dati a livello infrastrutturale con chiave di PSN.**

Block Storage Encrypted (500 GB) – SP PERFORMANCE

Il servizio è pensato per consentire la migrazione e la creazione di applicativi che non richiedono elevate prestazioni di accesso ai dati, come ad esempio **Web Application, FE, applicativi non mission critical, ambienti non produttivi.**

IaaS Storage (3/3)

OBJECT STORAGE ACTIVE - ARCHIVE

Il servizio Object Storage offre **soluzioni avanzate** per la **gestione, protezione e archiviazione dei dati** in modalità oggetti.

La **modalità Archive** è progettata per, **l'archiviazione a lungo termine** ideale per grandi volumi di dati che non richiedono accesso frequente, con funzionalità di versioning, metadati e sicurezza.
La **modalità Active** integra **policy WORM** (Write Once, Read Many), garantendo l'immutabilità dei dati e proteggendoli da cancellazioni accidentali o maliziose, con gestione centralizzata e funzioni avanzate di compliance.
Entrambi i servizi sono basati su infrastruttura dedicata e progettati per garantire elevata affidabilità, sicurezza e controllo completo sui dati.

OBJECT STORAGE ARCHIVE

- **Archiviazione di oggetti:** Consente di caricare, scaricare e gestire oggetti di qualsiasi dimensione.
- **Metadati:** Permette di associare metadati agli oggetti per facilitarne la ricerca e l'organizzazione.
- **Versioning:** Consente di creare e gestire diverse versioni dello stesso oggetto.
- **Sicurezza:** Offre funzionalità di sicurezza di base, come la crittografia dei dati a riposo e in transito.



OBJECT STORAGE ACTIVE – POLICY WORM

- **Immutabilità dei dati** per la durata configurata (conformità legale e tecnica)
- **Gestione eccezioni** controllata via console Snapshot e clonazione immutabili per garantire integrità e sicurezza dei dati
- **Protezione da cancellazioni** accidentali o maliziose
- **Gestione centralizzata** delle policy con console unificata e report dettagliati
- **Dati replicati** su più dispositivi per alta disponibilità e durabilità

Sistemi Operativi



VN = virtual node

L'accesso all'ecosistema Red Hat Enterprise Linux, lo standard di riferimento per i sistemi operativi in ambito enterprise, avviene attraverso un **processo strutturato** che consente di attivare le licenze e i servizi più adatti a ogni specifica esigenza infrastrutturale.

L'offerta è progettata per coprire l'intero ciclo di vita e tutte le necessità operative, includendo:

- **Licenze del Sistema Operativo base** (Red Hat Enterprise Linux), disponibili per ogni modello di deployment – da nodi fisici (Bare Metal) a macchine virtuali di ogni dimensione (Small, Large, XLarge).
- **Versioni ottimizzate per carichi di lavoro specifici**, come Red Hat Enterprise Linux for SAP Applications, per garantire massime performance e supporto certificato.
- **Strumenti di gestione centralizzata** come Red Hat Satellite, per governare in modo efficiente il ciclo di vita di intere flotte di sistemi.
- **Add-On per funzionalità avanzate**, tra cui l'Alta Disponibilità (**High Availability**), per assicurare la massima resilienza dei servizi critici.

Questo approccio strutturato garantisce la piena conformità delle licenze e fornisce l'accesso a una piattaforma enterprise sicura, gestita e pronta per supportare le applicazioni più strategiche della Pubblica Amministrazione.

Red Hat Enterprise Linux - Private

- Servizio inerente alle licenze Red Hat per nodi Esxi.

Red Hat Enterprise Linux - VM

- SMALL (fino a 8 vCPU) Ambienti virtualizzati Privati
- LARGE (fino a 127 vCPU)
- XLARGE (più di 128 vCPU)

Red Hat Enterprise Linux for SAP BARE METAL

- DB (nodi baremetal)
- APPLICATION (ambienti virtualizzati privati)
- LINUX (licenze Red Hat Satellite per ambienti bare metal)

Red Hat Enterprise Linux for SAP DB

- SMALL
- LARGE
- XLARGE

Red Hat Enterprise Linux for SAP Application – VM

- SMALL (fino a 8 vCPU)
- LARGE (fino a 127 vCPU)
- XLARGE (più di 128 vCPU)
- PRIVATE (ambienti virtualizzati privati)

Red Hat Enterprise Linux High Availability - Add-On

- Physical or VN, Dedicated, Yearly
- 1 to 8 vCPUs per VN, Multi-Tenant, Yearly
- 9 to 127 vCPUs per VN, Multi-Tenant, Yearly
- 128 to unlimited vCPUs per VN, Multi-Tenant, Yearly

Red Hat Satellite for Service Providers

- Full Support (Socket-Pair, Yearly)
- Full Support (Managed Node, Yearly)

Windows Server 2022

- Datacenter: 8 Core License Pack 1 Year
- Datacenter: 2 Core License Pack 1 Year
- Standard: 8 Core License Pack 1 Year

Networking

Il portafoglio Networking del PSN offre una suite completa di servizi per garantire connettività sicura, performante e flessibile per ogni scenario, dall'on-premise al multi-cloud.

1. Interconnessione Strategica:

Cloud Interconnect: Semplifica le migrazioni verso il PSN estendendo la rete locale (L2 su L3), senza richiedere modifiche agli indirizzi IP delle applicazioni.

Multi Cloud Interconnect: Fornisce accesso diretto e a bassa latenza ai principali cloud pubblici (Google, Azure, etc.) per architetture ibride.

2. Ottimizzazione ed Erogazione Applicativa:

L7 Load Balancer: Distribuisce il traffico in modo intelligente e sicuro, includendo funzionalità avanzate come WAF e gestione dei certificati SSL.

DNS: Servizio gestito (PaaS) per la risoluzione dei nomi all'interno del PSN, con server dedicati e console per la gestione autonoma.

3. Connettività Essenziale:

IP Pubblico Singolo: Un servizio semplice e diretto che fornisce un singolo indirizzo IPv4 pubblico. È la soluzione ideale ed efficiente per esporre su Internet un servizio specifico, superando la scarsità di indirizzi IPv4 disponibili.

Connettività e Interconnessione

Cloud Interconnect → interconnessione tra ambienti PSN/on-prem e supporto migrazione applicativa

Multi Cloud Interconnect → punto di interscambio strategico per connettere PSN con i principali CSP (Google Cloud, Azure, altri)

IP Pubblico Singolo → allocazione ottimizzata di indirizzi IPv4 per applicazioni pubblicate su internet

Naming e Risoluzione DNS

DNS → gestione DNS interno al PSN, con possibilità di forwarding verso DNS pubblici e piena autonomia per il cliente.

Servizi di Rete Avanzati

L7 Load Balancer (regional)→ bilanciamento intelligente del traffico (Layer 4/7), WAF integrato, TLS offload, scalabilità automatica

Security (1/4) - Protezione dell'Infrastruttura di Rete e delle Applicazioni

La sicurezza del perimetro e delle applicazioni si basa su un approccio stratificato, dove ogni servizio offre un livello di protezione specifico e complementare:

Next-Generation Firewall (NGFW) Premium: Evolve la protezione di rete tradizionale consentendo policy di sicurezza più granulari e precise.

Web Application Firewall (WAF): Servizio PaaS per proteggere le web app esposte su Internet. Difende automaticamente da attacchi informatici (come quelli OWASP o zero-day) e minimizza gli impatti legati allo sfruttamento di vulnerabilità note nel codice. Integrato con l'infrastruttura Industry Standard, può gestire anche dati di livello strategico. Disponibile in più taglie su **tecnologia Fortinet**, in base al traffico da proteggere.

Intrusion Prevention System (IPS): Analizza il traffico di rete in tempo reale e blocca attivamente le intrusioni e le minacce (sia note che sconosciute) prima che possano causare danni all'infrastruttura.

Perimeter Security Intelligence: Rende gli altri sistemi di difesa più efficaci nella prevenzione e monitoraggio delle emergenti minacce cyber.

NGFW

- NGFW platform
- NGFW platform - PaaS Upgrade

IPS

- Intrusion Prevention System (IPS)



PERIMETER SECURITY INTELLIGENCE

- Perimeter Security Intelligence

WAF

- Risorse Dedicate SMALL
- Risorse Dedicate (MEDIUM)
- Risorse Dedicate LARGE
- Risorse Dedicate (SMALL) PaaS Upgrade

Security (2/4) - Protezione di Dati, Endpoint e Posta Elettronica

Questa suite di servizi offre una protezione integrata per il patrimonio informativo, agendo sulla sicurezza dei dispositivi **(endpoint),** sulla visibilità dei dati e sulla difesa attiva dei contenuti.

Endpoint Protection (EPP): Fornisce una protezione avanzata per tutti i dispositivi, inclusi client, server e apparati specializzati IT/OT.

Data Security Posture Management (DSPM): Utilizza l'intelligenza artificiale per scoprire e classificare automaticamente i dati sensibili, fornendo la visibilità necessaria per garantire sicurezza e conformità alle normative sulla privacy.

Sicurezza Avanzata per File e Dati: Offre una piattaforma sicura (sandbox) all'interno del perimetro del PSN per analizzare file potenzialmente malevoli senza rischi.

Mail Security: Protegge il canale email bloccando minacce come phishing e ransomware prima che raggiungano gli utenti finali.

Key Vault / Key Management: Offre un vault sicuro per la gestione centralizzata delle chiavi crittografiche, dei segreti e dei certificati che proteggono i dati.



ENDPOINT PROTECTION IT/OT

Protezione completa di dispositivi e rete IT/OT

- Endpoint Protection IT/OT – Premium
- Endpoint Protection IT/OT – Standard
- Endpoint Protection – PaaS Upgrade
- EPP (IT)



SICUREZZA E GOVERNANCE DEL DATO

Visibilità sui dati sensibili e compliance

- DSPM (Data Security Posture Management)
- Key Vault as a Service
- DLP (Data Loss Prevention)



PROTEZIONE ATTIVA DEI CONTENUTI

Analisi sicura dei file, protezione del perimetro dati

- Sicurezza Avanzata per File e Dati
- Mail Security & Ransomware Protection

Security (3/4) - Gestione delle Identità e Controllo degli Accessi (Zero Trust)

Con l'aumento del lavoro da remoto e l'uso di servizi cloud, il tradizionale perimetro di rete è scomparso.

Oggi, il vero perimetro da difendere è l'identità digitale di ogni utente e dispositivo. Questa suite di servizi costruisce un **sistema di controllo robusto e moderno**, basato sul principio di concedere la minima fiducia possibile e di verificare sempre ogni richiesta di accesso.



L'integrazione di questi quattro servizi consente di costruire un'architettura di sicurezza resiliente e moderna, basata sulla filosofia "Zero Trust", dove ogni richiesta di accesso viene sempre verificata.

IDENTITY & ACCESS MANAGEMENT (IAM)

- **L'Identity & Access Management (IAM)** è il servizio fondamentale che centralizza e governa tutte le identità digitali dell'organizzazione. Si integra con sistemi esistenti (come Active Directory) per definire con precisione i permessi di accesso ("chi può fare cosa") e per semplificare l'esperienza utente attraverso il **Single Sign-On (SSO),** garantendo un accesso unificato e sicuro a tutte le applicazioni.

STRONG AUTHENTICATION

- La **Strong Authentication** garantisce la certezza dell'identità, aggiungendo un secondo livello di verifica oltre alla password. Utilizza meccanismi di **autenticazione multi-fattoriale (MFA)** – come codici temporanei (OTP), biometria o certificati digitali – per rendere l'accesso agli account significativamente più sicuro e resistente al furto di credenziali.

PRIVILEGED ACCESS MANAGEMENT (PAM)

- **Il Privileged Access Management (PAM)** è la soluzione specifica per la messa in sicurezza degli account con privilegi elevati, i più critici e a rischio. Il servizio centralizza le credenziali amministrative in un **vault protetto,** monitora e registra le sessioni per fini di audit e assegna i permessi in modo puntuale e controllato. Questo approccio previene abusi e attacchi mirati, garantendo al contempo la conformità alle normative.

ZERO TRUST NETWORK ACCESS (ZTNA)

- **Lo Zero Trust Network Access (ZTNA)** è il modello evoluto per l'accesso remoto sicuro, che supera i limiti delle VPN tradizionali. Invece di dare accesso all'intera rete, lo ZTNA concede l'accesso a **specifiche applicazioni** e solo dopo aver verificato sia l'identità dell'utente, sia la **postura di sicurezza del suo dispositivo** (es. antivirus, OS aggiornato). Se i controlli non sono superati, l'accesso viene negato, applicando il principio "mai fidarsi, verificare sempre"

Security (4/4) - Analisi Proattiva e Resilienza Operativa

Questa suite di servizi avanzati sposta il focus dalla semplice difesa alla gestione proattiva del rischio e alla resilienza. L'obiettivo è fornire gli strumenti per anticipare le minacce, avere una visione completa del proprio stato di sicurezza e garantire la capacità di recupero anche in caso di incidenti gravi.

Per scoprire le vulnerabilità: Il servizio di **Penetration Test Automatizzati** esegue test continui sull'infrastruttura per identificare i punti deboli prima che vengano sfruttati, fornendo un chiaro piano di azione per la loro risoluzione.

Per avere una visione d'insieme: Il **Cyber Situational Awareness** System agisce come una piattaforma di "comando e controllo", aggregando i dati da tutte le altre fonti di sicurezza (SIEM, EDR, etc.) per permettere analisi rapide e decisioni informate.

Per garantire la ripartenza: Il **Cyber Recovery and Vault (CRV)** protegge i dati e le applicazioni più critiche in un "vault" isolato e immutabile, al sicuro da attacchi ransomware, per assicurare un recupero rapido e affidabile dei servizi essenziali dopo un disastro.



PENETRATION TEST AUTOMATIZZATI

- verifica continua delle vulnerabilità

CRV

- protezione e recupero dei dati in caso di attacco ransomware/shock sistemici

CSAS

- visibilità strategica e operativa sulla sicurezza informatica

PaaS DB (1/3) - Piattaforma Database Oracle



Questa suite di servizi PaaS è dedicata all'ecosistema Oracle, progettata per supportare i **carichi di lavoro più critici e transazionali**. L'offerta garantisce massima performance e scalabilità attraverso infrastrutture specializzate come **Oracle Exadata** e **Alloy**, con il vantaggio di una piattaforma localizzata e conforme ai requisiti di sovranità digitale.

La flessibilità è assicurata dalla possibilità di scegliere tra **licenze incluse nel servizio o l'utilizzo di licenze proprie** (Bring Your Own License - BYOL), oltre a opzioni avanzate di alta affidabilità e disaster recovery.

Servizi inclusi:

PAAS ORACLE SU EXADATA / ALLOY

- **PaaS SQL** - Oracle DBMS EE (on EXA) (con licenza inclusa)
- **PSN Exadata Database Service** – Enterprise (su piattaforma Alloy)
- **PSN Exadata Database Service** - BYOL (su piattaforma Alloy)
- **PaaS SQL** - Oracle DBMS EE (on EXA) - BYOL

PAAS ORACLE SU X86

- **PaaS SQL** - Oracle DBMS SE (on x86) – BYOL
- **PaaS SQL** - Oracle DBMS EE (on x86) - BYOL

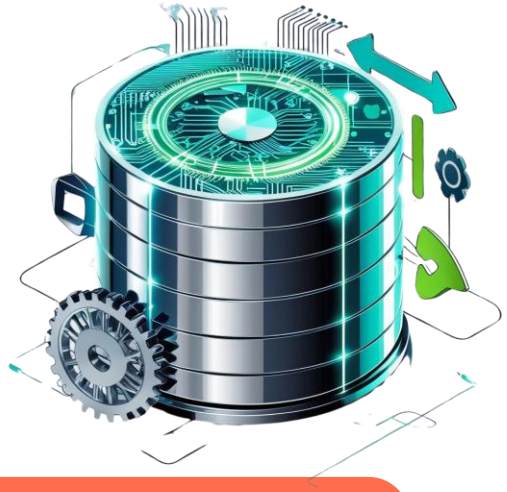
OPZIONI DI RESILIENZA E STORAGE

- **Alta Affidabilità (HA):** Read Replica con Active Data Guard (disponibile per Exadata, con e senza BYOL)
- **Disaster Recovery (DR):** Replica su Regione Secondaria (disponibile per Exadata e x86, con e senza BYOL)
- **PSN Exadata Database Service**: Storage (Storage aggiuntivo per Alloy)

PaaS DB (2/3) - Piattaforma Database SQL (Commerciali & Open Source)

Per offrire la massima libertà di scelta tecnologica, questa famiglia di servizi PaaS supporta i più diffusi database relazionali alternativi a Oracle. Include sia soluzioni commerciali enterprise come **Microsoft SQL Server**, sia i più affidabili e performanti database **open source** del mercato come **PostgreSQL, MySQL e MariaDB.**

Tutti i servizi sono erogati su un'infrastruttura moderna e ottimizzata (Hypershift) per garantire performance e stabilità.



Servizi inclusi:

MICROSOFT SQL SERVER

- PaaS SQL - MS SQL Server EE (con licenza inclusa)
- PaaS SQL - MS SQL Server EE (HA)
- PaaS SQL - MS SQL Server EE (BYOL)
- PaaS SQL - MS SQL Server EE in HA (BYOL)
- MS SQL Server EE - PaaS Upgrade

DATABASE OPEN SOURCE (TUTTI IN ALTA AFFIDABILITÀ - HA)

- PaaS SQL - PostgreSQL (HA)
- PaaS SQL - MySQL (HA)
- PaaS SQL – MariaDB (HA)
- MySQL - PaaS Upgrade

RISORSE COMUNI

- PaaS SQL - Risorse Storage addizionali

PaaS DB (3/3) - Piattaforma Database NoSQL & In-Memory

Questa suite di servizi PaaS è progettata per le esigenze delle applicazioni moderne, che richiedono altissima velocità, scalabilità orizzontale e la capacità di gestire dati non strutturati.

Include soluzioni **In-Memory** come Redis per caching, session store e applicazioni real-time, e database **NoSQL** come **MongoDB,** ideali per applicazioni web, mobile e per la gestione di dati non strutturati e semi-strutturati.

L'infrastruttura sottostante (Hypershift) è ottimizzata per basse latenze e alti carichi.

Servizi inclusi:

Database NoSQL a Documenti (MongoDB)

- PaaS NoSQL - MongoDB EE
- PaaS NoSQL - MongoDB EE (HA)
- MongoDB EE - PaaS Upgrade



Database In-Memory (Redis)

- PaaS In Memory – Redis
- PaaS In Memory - Redis (HA)

Middleware (1/2) - Piattaforme Applicative e di Esecuzione (PaaS)



Questa famiglia di servizi PaaS fornisce le piattaforme gestite e gli ambienti di esecuzione per accelerare lo sviluppo e la delivery di ogni tipo di applicazione. L'offerta copre l'intero spettro delle architetture moderne, liberando l'Amministrazione dalla gestione dell'infrastruttura sottostante.

Jboss as a Service: Offre un runtime gestito basato su WildFly per robuste applicazioni enterprise basate su tecnologia Java EE.

Spring boot as a Service: Mette a disposizione una piattaforma ottimizzata per lo sviluppo e l'esecuzione di moderni microservizi e applicazioni Java standalone.

Function as a Service (FaaS): Permette di eseguire singole funzioni di codice in modalità serverless, in risposta a specifici eventi, senza gestire l'infrastruttura.

PaaS CMS as a Service: La soluzione pronta all'uso, basata su WordPress, per la creazione e gestione rapida di siti web e portali istituzionali.

Red Hat Runtime Subscription: Servizio add-on che fornisce supporto tecnico enterprise, aggiornamenti e patch di sicurezza per le tecnologie Red Hat come JBoss.

RUNTIME PER APPLICAZIONI JAVA

- Jboss as a Service
- Spring boot as a Service

PIATTAFORMA SERVERLESS

- Function as a Service (FaaS)

PIATTAFORMA PER CONTENUTI WEB

- PaaS CMS as a Service
- CMSaaS - PaaS Upgrade

SUPPORTO TECNICO (ADD-ON)

- Red Hat Runtime Subscription

Middleware (2/2) - Piattaforme di Integrazione e Automazione

Questa suite di servizi PaaS agisce come il "sistema nervoso centrale" dell'infrastruttura digitale, fornendo gli strumenti avanzati per far funzionare le diverse applicazioni come un sistema unico, coeso ed efficiente.

API Management Platform: Governa e protegge l'intero ciclo di vita delle API, assicurando una comunicazione sicura e controllata tra le diverse applicazioni.

Business Process as a Service: Permette di disegnare, automatizzare e monitorare i processi di business, trasformando attività manuali in flussi di lavoro digitali.

PaaS ETL (Extract, Transform, Load): Offre un ambiente visuale per estrarre, trasformare e caricare dati da molteplici fonti, rendendoli pronti per l'analisi o l'utilizzo da parte di altre applicazioni.

Servizi inclusi:

INTEGRAZIONE E LA LAVORAZIONE DEI DATI (ETL):

- PaaS ETL - Batch / Real Time Processing

AUTOMAZIONE PROCESSI BUSINESS:

- Business Process as a Service (basato su tecnologia IBM)

GESTIONE DI API:

- API Management Platform

Data Protection (1/2) - Protezione dei Dati e Ripristino Operativo (Backup as a Service)

Il servizio di **Backup as a Service (BaaS)** è la soluzione fondamentale per la protezione e il ripristino dei dati della Pubblica Amministrazione.

Copertura Completa: Protegge i dati in ogni ambiente, sia cloud (PaaS, IaaS, PSN Managed) sia on-premise.

Flessibilità: Offre la scelta tra policy di backup standard gestite o configurazioni personalizzate con differenti periodi di conservazione (retention).

Sicurezza Avanzata: Include l'opzione **"Golden Copy"** per creare copie dei dati più critici immutabili e a prova di manomissione.

Obiettivo Finale: Garantire la continuità operativa dei servizi pubblici attraverso un ripristino rapido e sicuro da guasti, errori o cancellazioni.

BACKUP PER PIATTAFORME GESTITE E PAAS

- PSN Backup Service di Alloy
- Backup - PLATFORM (per personalizzare policy su PaaS DB)
- Backup per VM - PaaS Upgrade

BACKUP PER AMBIENTI ON-PREMISE

- Backup on PSN site (backup di dati on-premise verso il PSN)



PROTEZIONE AVANZATA DEL BACKUP

- PSN Golden Copy Service di Alloy (creazione di copie immutabili)

Data Protection (2/2) - Continuità Operativa e Cyber Resilience (DR & Protection scan)

Questa suite di servizi garantisce la continuità operativa e la **cyber-resilienza contro ogni tipo di incidente**, fornendo vari livelli di protezione complementari:

Disaster Recovery (DR): Assicura la rapida ripartenza dei servizi in un sito secondario in caso di disastro o indisponibilità del sito primario.

Protection Scan for Backup: protezione avanzata dei dati di backup contro i cyber-attacchi, eseguendo una scansione di sicurezza e creando copie isolate e immutabili in un vault per un ripristino rapido e sicuro (soluzione Threat Scan di Commvault).

Il servizio è disponibile in **due versioni dedicate:** una per **l'ambiente Industry Standard** e una specifica per l'ambiente **PSN Managed (Oracle Alloy).**

Servizi inclusi:

Disaster Recovery (DR)

- Opzione DR (da on-premise a sito PSN)
- Opzione DR (tra siti PSN per VM e PaaS DB)
- Opzione DR con Test una-tantum incluso



Protection Scan for Backup

- Protection Scan for Backup (scansione anti-malware dei backup

Infra & OPS Platform (1/2) - Piattaforme per la Gestione dei Servizi e delle Operation IT

Questa famiglia di servizi fornisce il **sistema nervoso centrale per un'organizzazione IT moderna**, offrendo piattaforme integrate per governare i processi, monitorare le infrastrutture e gestire le operation.

Attraverso soluzioni leader di mercato, consente di automatizzare la gestione di richieste, incident e change, garantendo al contempo una visibilità costante sulle performance e lo stato di salute dei workload.

L'obiettivo è aumentare l'efficienza, migliorare la qualità dei servizi erogati e assicurare la resilienza operativa.

Servizi inclusi:

Piattaforme di IT Service Management (ITSM) e Ticketing

- PaaS Servizio di Ticket Management (basato su Atlassian JIRA)
- PaaS Servizio di Ticket Management (basato su ServiceNow ITSM)
- PaaS Servizio di Operations Management (basato su BMC Helix ITSM)
- Add-On: ServiceNow ITOM
- Add-On: Discovery Item (per BMC Helix)



Monitoraggio e Logging Infrastrutturale

- IT Infrastructure Service Operations (Logging & Monitoring)

Infra & OPS Platform (2/2) - Piattaforme di Controllo Strategico e Gestione Multi-Cloud

Questa suite di servizi permette alle amministrazioni di avere un **controllo strategico e una governance completa** su ambienti complessi, distribuiti su più cloud e domini operativi. Dalla gestione multi-cloud al monitoraggio in tempo reale di scenari operativi complessi **(Control Room)**, le piattaforme garantiscono visibilità unificata, automazione e capacità di orchestrazione, essenziali per supportare i moderni percorsi di trasformazione digitale.

A questo si affiancano soluzioni avanzate di ***Situational Awareness***, capaci di aggregare e analizzare dati da fonti eterogenee (IT e OT) per fornire un supporto decisionale completo in scenari operativi critici.

Servizi inclusi:

Piattaforme di Gestione Multi-Cloud

- Multicloud Management Platform (Leonardo – Secure Cloud Management Platform)
- Multicloud Management Platform (Morpheus)
- Multicloud Management Platform – PaaS Upgrade



Control Room e Situational Awareness

- Control Room as a Service (piattaforma di aggregazione e analisi multi-sorgente)

DevSecOps - Software Quality Platform

Questa **suite di servizi PaaS** supporta la Pubblica Amministrazione nell'adozione di pratiche **DevSecOps** e di sviluppo software sicuro e di qualità.

Le soluzioni coprono l'intero ciclo di vita applicativo — **dall'automazione della configurazione** e dei test, alla gestione integrata di **pipeline CI/CD**, fino al controllo continuo della qualità del codice e alla sicurezza applicativa.

Un approccio moderno per abilitare delivery continua, qualità del software e sicurezza by design, in linea con le best practice internazionali.

Servizi inclusi:

Automation & CI/CD

- DevSecOps as a Service by PSN (CI/CD pipeline + versioning + build + release - Piattaforma centrale basata su GitLab)
- Configuration Manager (Basato su Red Hat Ansible Automation)
- Test Automation
- Test Automation – PaaS Upgrade



Security & Code Quality

- Qualizer DevSecOps (Piattaforma avanzata di sicurezza DevSecOps)
- Quality Code Analysis (analisi statica della qualità del codice)

BigData e AI (1/2) - Piattaforme Dati e Modelli Fondazionali AI

Questi servizi sono come un **laboratorio tecnologico completo**. Forniscono gli strumenti e le materie prime per chi vuole costruire le proprie soluzioni personalizzate di analisi e Intelligenza Artificiale.

Includono sia le piattaforme per la gestione dei dati – come il **Data Lakehouse** (un archivio unico, sicuro e organizzato per conservare ogni tipo di dato) e la **Business Intelligence** (per esplorare i dati e creare report) – sia i "motori" grezzi dell'AI. Questi "motori", come i **Modelli Linguistici (LLM)**, non sono applicazioni finite, ma sistemi potenti che possono essere addestrati e adattati per creare soluzioni uniche, ad esempio un assistente virtuale che comprenda il linguaggio specifico di un'amministrazione.

Servizi inclusi:

Piattaforme Dati e Analytics

- Data Lakehouse (basato su Cloudera Data Platform)
- Business Intelligence Platform (basato su Microsoft Power BI)
- AI Workflow (basato su KNIME)



Componenti per lo Sviluppo di AI Generativa

- AI LLM Italy (Modello linguistico bilingue)
- AI SLM (Modelli linguistici compatti)
- AI Search - RAG (per ricerca contestualizzata)
- Vector DB (Database per ricerca vettoriale)

BigData e AI (2/2) - Servizi Cognitivi e API di Intelligenza Artificiale

Questa suite di servizi mette a disposizione funzionalità di Intelligenza Artificiale avanzate e "pronte all'uso", accessibili tramite semplici interfacce **API** per una facile integrazione in qualsiasi applicazione.

Permettono di arricchire istantaneamente i processi con la capacità di comprendere il mondo non strutturato: dalla **trascrizione automatica della voce (Speech to Text)** e la **lettura di documenti e immagini (OCR)**, fino alla **traduzione multilingua** e all'**estrazione di dati da moduli e fatture (Text Analytics).**

L'obiettivo è accelerare l'innovazione, automatizzare le attività manuali e migliorare l'efficienza e la qualità dei servizi offerti ai cittadini.

Servizi inclusi:

Analisi di Linguaggio e Audio

- Speech to Text (Trascrizione Vocale)
- Translation (Traduzione Neurale)



Analisi di Immagini e Documenti

- OCR (Riconoscimento Ottico dei Caratteri)
- Text Analytics (Estrazione Dati da Documenti)

VDI e Instant messaging -

Questa suite di servizi è progettata per abilitare lo **Smart Working** e creare un **Digital Workplace** moderno, sicuro e flessibile per la Pubblica Amministrazione.

L'offerta si basa su due pilastri fondamentali e complementari: da un lato, la **Virtual Desktop Infrastructure (VDI)**, che fornisce un ambiente di lavoro personale e sicuro accessibile da qualsiasi dispositivo; dall'altro, una piattaforma di **Instant Messaging e Collaborazione**, che offre gli strumenti per comunicare e lavorare in team in modo efficace e protetto.

Servizi inclusi:

Il Posto di Lavoro Virtuale (VDI)

- VDI Completa (desktop virtuale standard personalizzabile)
- VDI con supporto a GPU (per carichi di lavoro con grafica avanzata)
- Erogazione di VDI - PaaS Upgrade (per deployment su infrastruttura esistente)



La Collaborazione in Tempo Reale (Instant Messaging)

- Instant Messaging - BASIC (Piattaforma sicura basata su Mattermost)

Supporto Premium (1/2)

Descrizione servizio

- Il Servizio di supporto Premium, nasce dall'esigenza espressa dai grandi clienti (VIP) di poter usufruire di un **servizio specialistico dedicato H24**, che possa garantire un **supporto diretto**, **integrato** e **continuativo** per tutta la durata della fase di esercizio. Il personale che risponde alla PA tendenzialmente è lo stesso
- Servizio erogato in proattività/reattività ed è diviso su questi livelli:
  - **Front End**: raccoglie tutte le richieste cliente, effettua il triage ed interviene per perimetro di competenza. In caso di problematiche e/o necessità di competenze specialistiche ingaggia i **Service Matter Expert e/o Technology Matter Expert**
  - **Back End**: con competenze specifiche e verticali sia lato servizi offerti alla specifica PA e relative catene ed architetture applicative (Service Matter Expert) sia sulle componenti middleware/infrastrutturali/prodotto/rete (Technology Matter Expert). È **organizzato per aree verticali** al fine di mappare le **principali tecnologie e architetture utilizzate dalla PA**. Coordina e gestisce gli interventi di eventuali terze parti (ad esempio specifico vendor tecnologico) e supporta le attività di setup degli ambienti e di migrazione, in coordinamento con gli eventuali Enabler.

Dimensionamento

- Dimensionato sulla base del numero di **Sistema Gestito Normalizzato (SGN).** L'unità di misura adottata per rappresentare la complessità delle infrastrutture IT monitorate e gestite**. Per determinare il numero di SGN ci si può avvalere dello strumento di simulazione di TIM** che richiede in input elementi tipo il #vCPU, # DB, # stack applicativi ecc.
  - A listino sono presenti **4 SKU da usare** in base alla **famiglia di servizio attivata dal cliente** (industry standard, secure public cloud, PaaS Hybrid, PSN managed)

Supporto Premium (2/2) - SLA

ID	Descrizione KPI	Orario di servizio	SLA	KPO	Freq. di misurazione
K.PRMCS.PX	Tempo massimo di presa in carico Incident Priorità P1,P2 e P3	H24	<= 10 minuti	>=97% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.P1	Tempo di evasione degli incident di gestione di priorità P1 (*)	H24	<= 1 ora	>=80% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.P2	Tempo di evasione degli incident di gestione di priorità P2	H24	<= 3 ore	>=90% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.P3	Tempo di evasione degli incident di gestione di priorità P3	H24	<= 4,5 ore	>=90% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.CHANGE.P1	Tempo per l'esecuzione della Change sui servizi infrastrutturali per i servizi Critici	Lun. - Ven. 08:00 - 17:00 giorni lavorativi	<= 4 ore	>=90% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.CHANGE.P2	Tempo per l'esecuzione della Change sui servizi infrastrutturali per i servizi Standard	Lun. - Ven. 08:00 - 17:00 giorni lavorativi	<= 24 ore	>=90% (applicabile su min 10 ticket nel periodo di osservazione)	trimestrale
K.PRMGI.CHANGE.P3	Tempo per l'esecuzione della Change sui servizi infrastrutturali per i servizi Base	Lun. - Ven. 08:00 - 17:00 giorni lavorativi	<= 72 ore	>=90% (applicabile su min 10 ticket nel periodo di osservazione)	Trimestrale
K.PRM.TURNOVER	Tasso di Turnover del personale impiegato	N/A	<=30%	Al raggiungimento di una soglia di turn-over del **30%** del team si provvederà a convocare un incontro con la PA al fine di adottare misure di remediation condivise	Semestrale

Ulteriori aggiornamenti di listino

Aggiornamenti avvenuti nel corso del 2026

I servizi aggiunti a listino rientrano nelle seguenti categorie di offerta, di cui vengono forniti maggiori dettagliati nei capitoli successivi:

1. Secure Public Cloud Oracle

Secure Public Cloud Oracle

Il Secure Public Cloud Oracle estende il perimetro dell'offerta PSN, introducendo nuovi servizi e capacità rispetto al modello Public Cloud Managed.

Consente di accedere a un ecosistema OCI più ampio, superando vincoli tecnologici e mantenendo il modello di sicurezza PSN.

1. Estensione dell'offerta Secure Public Cloud di Psn con tecnologia Oracle Cloud Infrastructure

Disponibilità di servizi e capability Oracle Cloud Infrastructure nell'ambito dell'offerta Secure Public Cloud, securizzati per la gestione di dati critici che non richiedono gli ulteriori controlli operativi di sicurezza specifici dei servizi Public Cloud PSN Managed previsti per i dati strategici

2. Introduzione di tecnologie Oracle avanzate

Accesso a componenti aggiornati ed evoluti:

- Exadata di nuova generazione (X9M, X11M)
- nuove classi compute (E4, E5, E6)
- Object Storage avanzato (Archive, Infrequent Access)

3. Copertura estesa dei servizi OCI

Ampliamento sui principali domini tecnologici: Compute, Database, Storage, Networking, Security, AI e integrazione applicativa, aumentando i casi d'uso supportati.

4. Modello Secure Public Cloud PSN

Servizi erogati secondo il modello PSN, con:

- securizzazione dei tenant
- utilizzo del modello BYOK ove applicabile
- gestione centralizzata delle chiavi tramite KMS/HSM PSN

Agenda

1. INTRODUZIONE
2. CONTESTO DI RIFERIMENTO
3. POLO STRATEGICO NAZIONALE: PERCORSO, VANTAGGI E TECNOLOGIE
4. SOLUZIONI OFFERTE DA POLO STRATEGICO NAZIONALE
5. COME ADERIRE

- Step di adesione a Polo Strategico Nazionale
- Avvisi per migrazione a Polo Strategico Nazionale
- Piano di migrazione e attivazione servizi



Step di adesione a Polo Strategico Nazionale

DURATA CONVENZIONE: 13 ANNI

DURATA: 36 MESI

DURATA CONTRATTI: 10 ANNI

CONVENZIONE

24.8.2022

Convenzione tra Polo Strategico Nazionale e Dipartimento per la trasformazione digitale

22.12.2022

Attivazione Polo Strategico Nazionale: collaudo dell'infrastruttura

08.2025

Termine sottoscrizione contratti d'utenza PA - Polo Strategico Nazionale

2026

Perfezionamento migrazione delle Amministrazioni a Polo Strategico Nazionale

CLASSIFICAZIONE PIANI DI MIGRAZIONE

18.7.2022 (pror. 15.10.2022)

PA invia ad ACN la classificazione di dati e servizi

28.2.2023

PA invia piani di migrazione a DTD e ACN

2026

Completamento migrazione

Piano e progetto dei fabbisogni

La Convenzione stabilisce delle attività propedeutiche e tempistiche predefinite per la sottoscrizione dei contratti d'utenza con le Amministrazioni.



	PIANO DEI FABBISOGNI	PROGETTO DEL PIANO DEI FABBISOGNI	CONTRATTO D'UTENZA
LA PA	Predispone ed invia al PSN il **piano dei fabbisogni** che specifica l'esigenza dell'amministrazione in termini di perimetro IT da migrare verso il PSN e le tipologie di servizi richiesti come da catalogo	Resta in attesa della ricezione del **progetto del piano dei fabbisogni che il PSN è tenuto ad inviare entro 60 giorni**	Verifica il **progetto del piano dei fabbisogni** e richiede eventuali osservazioni entro 10 giorni Se il progetto è approvato, stipula il **contratto d'utenza** sulla base dello schema allegato alla Convenzione
PSN	Fornisce supporto alla PA per la redazione del **piano dei fabbisogni**	Invia alla PA il **progetto del piano dei fabbisogni** con la descrizione dei servizi e la relativa quantificazione economica. Allega inoltre il **piano di migrazione di massima**	In caso di osservazioni delle PA, aggiorna coerentemente il **progetto del piano fabbisogni** entro 10 giorni Se il progetto è approvato dalla PA, stipula il **contratto d'utenza**

Piano di migrazione e attivazione servizi

Le Amministrazioni saranno assistite lungo tutte le fasi, dall'onboarding fino al termine della Convenzione.



FASI	CONTRATTO D'UTENZA	NOMINA DEL PMCA E KICK OFF DI PROGETTO	PIANO DI MIGRAZIONE DI DETTAGLIO	OPZIONALE PIANO DI MIGRAZIONE DI DETTAGLIO REVISIONATO	ATTIVAZIONE DEI SERVIZI	CONTROLLO E SUPPORTO	CESSAZIONE
LA PA	L'Amministrazione utente nomina un Direttore dell'Esecuzione		**Opzionale – Invio osservazioni al Piano di Migrazione di dettaglio entro 10 giorni**	**Attivazione dei servizi con tempistiche definite nel piano di migrazione**	**Coadiuva le risorse del PSN nelle attività di deployment / testing** **Usufruisce dei servizi** (che può attivare, cambiare o disattivare) e attiva **supporto tecnico** del PSN in caso di necessità		
IL PSN	Il Concessionario nomina un Direttore del Servizio e un Referente del Servizio	**Presentazione del piano di migrazione** di dettaglio contenente le **macro attività** del servizio, come condiviso durante il kick off di progetto	In caso di osservazioni delle PA, aggiorna coerentemente il progetto del piano di migrazione entro 10 giorni	**Entro 36 mesi dalla sottoscrizione della convenzione – salvo diverso accordo tra concessionario e concedente**	Attiva l'erogazione dei servizi **garantendo continuità operativa, formazione** per la PA e **monitoraggio** della corretta **erogazione dei servizi**		

Vogliamo abilitare l'innovazione e la trasformazione digitale italiana attraverso la gestione sicura dei dati e dei servizi della Pubblica Amministrazione.

Polo Strategico Nazionale

Cloud sicuro per l’Italia digitale.

www.polostrategiconazionale.it

Quali cloud per la PA? L'importanza della qualificazione

La PA può acquistare solo servizi in cloud qualificati, che devono rispondere a specifici standard tecnico-organizzativi, misure di controllo sui dati, modalità di gestione delle chiavi di cifratura e controlli di sicurezza.

Sulla base dell'analisi delle soluzioni tecnologiche e organizzative disponibili sul mercato, sono state identificate **5 tipologie di servizi cloud**

CLASSIFICAZIONE SERVIZI CLOUD	CARATTERISTICHE	REQUISITI DI SICUREZZA	LOCALIZZAZIONE DEI DATI	GESTIONE OPERATIVA
PUBBLICO NON QUALIFICATO (EXTRA UE / UE)	Servizi di cloud pubblico non qualificati rispetto alle normative UE	REQUISITI DI SICUREZZA	EXTRA UE UE	CSP non qualificati
PUBBLICO (UE)	Servizi di Cloud pubblico qualificati rispetto alle normative UE	Controlli di sicurezza ordinari	UE	CSP qualificati
PUBBLICO CRIPTATO (IT)	Servizi di Cloud pubblico qualificati rispetto alle normative UE	Crittografia con controllo delle chiavi in Italia		
PRIVATO / IBRIDO "SU LICENZA" (IT)	Servizi di Cloud privato e ibrido qualificati con gestione delle chiavi in Italia		ITALIA	Fornitori soggetti a vigilanza e monitoraggio pubblico
PRIVATO (IT)	Servizi di Cloud privato qualificati mediante scrutinio tecnologico	Crittografia nazionale con controllo delle chiavi in Italia		

Il quadro normativo di riferimento

Polo Strategico Nazionale nasce per rispondere a specifiche **linee guida e norme** sulla **sicurezza** e la **sovranità** di dati e servizi delle Pubbliche Amministrazioni.

- **Legge 11/09/2020 n.120:** impegna la Presidenza del Consiglio dei Ministri allo sviluppo di un'infrastruttura ad alta affidabilità sul territorio nazionale per la razionalizzazione e il consolidamento dei Centri Elaborazioni Dati (CED).
- **Art. 33-septies D.L. n.179 del 18 ottobre 2012 (sostituito dal D.L. 76/2020):** decreta la migrazione di CED e servizi informatici delle Pubbliche Amministrazioni Centrali verso PSN, infrastrutture con requisiti ACN o soluzioni cloud secondo regolamento AgID (data center tipo A).
- **Art. 35 del D.L. n.76 del 16 luglio 2020:** promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale.
- **GDPR e Sentenza Schrems II:** precludono agli operatori di esportare il dato fuori dai confini europei.
- **Decreto Legge 21 settembre 2019, n. 105:** Disposizioni urgenti in materia di Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e relativi decreti attuativi
- **Legge 28 giugno 2024, n. 90:** Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici
- **Regolamento per le infrastrutture e i servizi cloud per la PA, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024:** individua le modalità per la classificazione, per la migrazione e per la qualificazione dei servizi cloud, di cui la PA può approvvigionarsi ricorrendo al libero mercato; riporta le misure e i requisiti per il raggiungimento dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA; elenca le caratteristiche di qualità, sicurezza, performance, scalabilità e portabilità dei servizi cloud per la PA.
- **Decreto legislativo 4 settembre 2024, n. 138 (NIS2):** recepimento nell'ordinamento nazionale della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione.

Qualifiche e certificazioni

Qualifiche ACN

(Decreto direttoriale n. 29 del 02/01/2023, requisiti di cui all'allegato 1 della determina n. 307 del 18 gennaio 2022)

- QI4 alla infrastruttura "'Infrastruttura Cloud PSN"
- QC4 al servizio IaaS "IaaS Private PSN"
- QC4 al servizio IaaS "'IaaS Shared PSN"
- QC4 al servizio IaaS \'CaaS PSN"
- QC4 al servizio PaaS "'DRaaS PSN"
- QC4 al servizio PaaS "BaaS PSN"
- QC4 al servizio PaaS "AI PSN"
- QC4 al servizio PaaS "BigData PSN"
- QC4 al servizio PaaS "PaaS IAM PSN"
- QC4 al servizio PaaS "DBaaS PSN"

La sicurezza dell'infrastruttura e dei servizi PSN è comprovata da numerose certificazioni e risponde ai massimi standard di sicurezza

- ISO/IEC 27001 Sistema di gestione della Sicurezza delle Informazioni
- ISO/IEC 27017 Sistema di gestione della Sicurezza delle Informazioni per i servizi nel Cloud
- ISO/IEC 27018 Sistema di gestione della Sicurezza delle Informazioni per i dati personali nei Servizi Cloud
- ISO/IEC 27035-1 e ISO/IEC 27035-2 Gestione degli incidenti di Sicurezza
- ISO/IEC 27701 Specifica delle Informazioni sulla Privacy
- ISO/IEC 29100 Privacy framework
- ISO/IEC 22301 Business Continuity Management System
- ISO/IEC 9001 Quality Management System
- ISO/IEC 20000-1 Service Management
- ISO 14001 Sistema di gestione ambientale
- ISO 14064:2018 Gestione, rendicontazione e verifica di dati ed informazioni riferiti ai GHG (GHG -Greenhouse gases, gas ad effetto serra)
- ISO 45001:2018 Sistema di gestione per la salute e sicurezza sul lavoro (SSL)
- ISO 37001:2016 Anti corruzione
- ISO 50001 Sistema di gestione dell'energia (SGE)
- ANSI/TIA-942 Rating 3/4 - Leed Gold Standard per affidabilità Datacenter
- ISO/IEC TS 22237 Data center facilities and infrastructures
- CSA Star Cloud Security Alliance – Star – Level2 - Audited