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

CUP: J51B21005710007

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

Ministero Della Difesa

2023-0000080248290589-PPdF-P1R2M1

SOMMARIO

Indice delle tabelle

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	*Revisione*	*Data*
Prima Emissione	*1*	*06/05/2025*
Seconda Emissione	*2*	*21/05/2025*

Tabella 1: Informazioni Documento

Autore:	
	TIM / LDO / Sogei

Tabella 2: Autore

Revisione:	
PSN Solution team	*n.a.*

Tabella 3: Revisore

Approvazione:	
Solution Design *PSN Commercial team*	*Andrea Tomei* *Diego Cavallero*

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

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

ESTERNA A:

- *Referente Contratto Esecutivo <Mitola Petruzzelli Walter.>*
  - *Email: < cra.contratti.infocom@smd.difesa.it.>*
  - *Tel: <INSERIRE TEL RIF. REFERENTE CONTRATTO ES.>*
- *Referente Tecnico <Golino Valerio>*
  - *Email: < sesto.dataman.cu@smd.difesa.it >*
  - *Tel: <3203622485>*
- *Referente di sicurezza <Golino Valerio>*
  - *Email: < sesto.dataman.cu@smd.difesa.it >*
  - *Tel: <3203622485>*

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del PSN relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012. Quanto descritto, è stato redatto in conformità alle richieste dello Stato Maggiore della Difesa di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (ID 2025-0000080248290589-PdF-P2R1) opportunamente analizzate e circoscritte alle attività previste dalla Convenzione PSN.

Il presente progetto dei fabbisogni risulta essere un'estensione dell'attuale contratto in esercizio tra il Ministero della Difesa ed il Polo Strategico Nazionale identificabile con il CIG numero A04AE447E0.

2 AMBITO

I principali obiettivi che l'Amministrazione della Difesa intende perseguire attraverso il presente Piano dei Fabbisogni riguardano:

- *la disponibilità di uno spazio Azure sul Secure Public Cloud del PSN per la migrazione graduale di servizi attualmente in esercizio presso le proprie articolazioni.*
- *Servizi di Sicurezza da attivare sull'infrastruttura Secure Public Cloud Azure.*

Di seguito, si riporta la tabella dei servizi Azure a catalogo attualmente identificati. Tale tabella potrà essere integrata di ulteriori servizi o modificata in alcune tipologie scelte in fase di redazione del Progetto dei Fabbisogni.

Il presente Progetto dei Fabbisogni richiede la predisposizione di un'infrastruttura su Secure Public Cloud basata su Microsoft Azure al fine di rendere disponibile un'ambiente di calcolo all'interno del quale verranno migrati specifici servizi, a scelta dell'Amministrazione. La migrazione del servizio specifico non è inclusa nel presente progetto che sarà pianificata in una fase successiva. Si riporta di seguito la classificazione dei dati prevista per le applicazioni di futura migrazione:

Nome servizio	*Classificazione ACN*
Piattaforma AI	*Ordinario*

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

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

Tabella 5 Documenti Contrattuali

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

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

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

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

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

3.2 DOCUMENTI DI RIFERIMENTO

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

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

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

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

Tabella 7: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
CMP	Cloud Management Platform
CSP	Cloud Service Provider
DR	Disaster Recovery
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
SCORM	Shareable Content Object Reference Model
VM	Virtual Machine
WBT	Web Based Training
BYOK	Bring Your Own Key
GCP	Google Cloud Provider
HSM	Hardware Security Module
TCB	Trusted Compute Bases
AZ	Availability Zone

Tabella 8: Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

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

5.1 SERVIZI PROPOSTI

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

Servizio	*Tipologia*
Microsoft Azure	*Secure Public Cloud*
Security Professional Services	*Servizi Professionali*

Tabella 9: Servizi Proposti

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

5.2 SECURE PUBLIC CLOUD

5.2.1 Descrizione del servizio

Il Secure Public Cloud è un servizio PSN Core che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza (Chiavi esterne, backup, template, servizi professionali).
L'architettura del servizio "Secure Public Cloud" è basata su due componenti principali:

- *Public Cloud: La componente Hyperscale Public Cloud, erogata da una Region collocata sul territorio nazionale, ai cui servizi vengono applicate configurazioni, policy e controlli di sicurezza, al fine di garantire ai clienti ambienti di elaborazione segregati aventi una sicurezza di base adeguata agli scopi del PSN;*

- *Security & Governance: Una componente, erogata dai Data Center del PSN distribuiti sul territorio Nazionale, nella quale verranno configurati servizi atti a garantire l'adeguato livello di sicurezza dei servizi erogati sul Public Cloud (Gestione Chiavi e Backup).*

Tale scenario prevede la presenza dei seguenti attori:

- *Fornitore dei servizi di Public Cloud (CSP):*
  - *fornisce la piattaforma su cui è costruita la componente Hyperscale Public Cloud dell'architettura*
- *PSN:*
  - *si occupa di progettare, erogare, gestire e controllare i servizi cloud ed in modo particolare la componente di sicurezza e governo di base adeguati agli scopi del PSN;*
  - *fornisce servizi di sicurezza opzionali a "valore aggiunto" integrati ai servizi base tramite servizi professionali per la securizzazione.*

Il Secure Public Cloud è un servizio core del PSN che garantisce alti standard di sicurezza:
GESTIONE DELLE CHIAVI. Relativamente alla gestione delle chiavi la soluzione comprende:

- *Impiego di terze parti (e.g., Thales CipherTrust) con grande livello di autonomia nella gestione delle chiavi crittografiche per soluzioni in cloud con il modello Bring Your Own Key (BYOK).*
- *Soluzione di key management replicata nei due datacenter HA e territorialmente nelle due Region.*
- *Controllo on-premise per ciascuna fase del ciclo vita delle chiavi, consentendo di eseguire in autonomia:*
  - *generazione delle chiavi ON-PREMISE tramite l'utilizzo di dispositivi crittografici certificati;*
  - *esecuzione dei backup delle chiavi;*
  - *installazione diretta delle chiavi sui Key Vault in cloud;*
  - *monitoraggio degli accessi alle chiavi;*
  - *rotazione manuale o periodica delle chiavi;*
  - *revoca delle chiavi.*
- *On-Prem HSM certificato FIPS 140-2 L3 con partizioni multiple per la corretta gestione del materiale crittografico (chiavi simmetriche ed asimmetriche, generazione entropia, ..).*
- *CipherTrust Manager per la gestione del ciclo di vita delle chiavi on-premise e in Cloud.*
- *CipherTrust Cloud Key Manager come orchestratore dei processi di gestione delle chiavi in Cloud. Generazione delle chiavi on-premise per importazione sicura sul cloud provider per tutto il ciclo di vita.*

GOVERNANCE MODEL. Per ogni cliente viene creato un ambiente standard segregato e auto-consistente in cui, tramite servizi di delega dei privilegi (ad esempio Azure Lighthouse e Privileged Identity Management) è possibile proiettare i servizi di monitoraggio e sicurezza dello specifico ambiente cliente verso l'ambiente del gestore del PSN che quindi avrà:

- *Visibilità di tutti gli ambienti*
- *Capacità di intervento automatizzato su larga scala*
- *Possibilità di enforcement delle policy definite*

I Privilegi di amministrazione sono disabilitati per default e vengono attribuiti agli operatori a valle di un processo di autorizzazione: questo meccanismo garantisce il mutuo controllo da parte del cliente e del provider con intrinseco innalzamento del livello di sicurezza.

Le caratteristiche di questo modello di gestione forniscono:

- *Gestione uniforme e standardizzata dei tenant cliente;*
- *Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, di set di regole di sicurezza predefinite in linea con best practices internazionali;*
- *Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, dei ruoli standard per ogni funzione (Ruoli PSN, Ruoli PA, Ruoli terze parti);*
- *Disponibilità di template securizzati ed integrati a strumenti di sicurezza;*
- *Gestione unificata dell'identità;*
- *Gestione degli eventi di sicurezza;*

CONFIDENTIAL COMPUTING. L'obiettivo del PSN è rafforzare il livello di confidenzialità e sicurezza del dato in uso tramite i seguenti metodi:

- *Ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations.*
- *Usare tecniche di enforcement basate su componenti tecnologiche piuttosto che su processi organizzativi.*
- *Fornire trasparenza sulle garanzie, i rischi residui e le mitigazioni che si possono implementare.*
- *I modelli di attacco contro le applicazioni cloud si basano su tecniche diverse per prendere di mira codice o dati in uso, ad esempio:*
    - *breakout di hypervisor e container;*
    - *compromissione del firmware ed altre minacce interne, ognuna delle quali si basa su tecniche diverse per prendere di mira codice o dati in uso.*

Confidential Computing (per VM, K8S, HSM) è la protezione dei dati in uso utilizzando ambienti di esecuzione attendibili basati su hardware

SOLUZIONI HUB & SPOKE. Per quanto riguarda l'ambiente Secure Public Cloud è previsto l'uso di un modello Hub & Spoke per consentire al PSN il controllo del traffico e la gestione delle DMZ per l'ambiente cloud.

Le Amministrazioni potranno creare reti virtuali spoke nei segmenti, dove saranno attive Policy che forzeranno la connessione con Virtual Network Hub e impediranno la creazione di tipologie di risorse controllate centralmente, come, ad esempio, gli indirizzi IP pubblici.

BACK UP. Per esercitare la sovranità del dato, il Secure Public Cloud prevede l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP tramite ulteriore livello di archiviazione.

Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup del PSN in modo che lo Storage su cui risiede il dato protetto sia gestito dal personale PSN.

L'integrazione prevede l'uso di tecniche di backup snapshot o stream-based e la cifratura dei dati "at rest" e in transito per garantire la protezione e il ripristino delle macchine virtuali a cui è rivolto il servizio, anche di quelle che implementano meccanismi di encryption del disco di sistema e dei dischi dati.

5.2.2 Personalizzazione del servizio

Nel corso della fornitura i fabbisogni, riportati nel Cap. 8 – Configuratore potranno essere adeguati/rivisti al manifestarsi di specifiche esigenze dell'Amministrazione.

Si specifica che ***l'avanzamento della fatturazione sarà in funzione dei consumi effettivi realizzati nel mese della soluzione Secure Public Cloud****.*
Tutte le licenze software sono messe a disposizione dall'Amministrazione. Ai sensi delle disposizioni di cui al presente PPdF l'Amministrazione Utente ha l'obbligo di garantire l'aggiornamento dei sistemi operativi e applicativi alle versioni più recenti (i.e. in support) e oggetto di migrazione sul PSN.
Si precisa che, nelle more dell'effettuazione di detti aggiornamenti da parte di Codesta Amministrazione Utente,

- *PSN provvederà alla fornitura dei servizi e non potrà esser ritenuto responsabile di eventuali disservizi e/o danni patiti dall'Amministrazione anche relativamente agli SLA di cui all'allegato H alla Convenzione.*

Si precisa, infine, che l'Amministrazione Utente si obbliga a procedere all'aggiornamento dei sistemi alle versioni più recenti, comunque, entro e non oltre 4 mesi dalla data di avvenuta migrazione, fermo restando che, in caso contrario, PSN non potrà garantire la regolare esecuzione dei servizi e precisando comunque che, fino all'effettivo aggiornamento degli stessi alle versioni in support, l'Amministrazione manleverà PSN da qualsivoglia danno, onere, spesa e costo in capo a se stessa, terzi e/o PSN che sia correlato al mancato aggiornamento dei sistemi.

Le capacità stimate sono in linea con quanto emerso durante la fase di analisi eseguita per la produzione di questo documento.

Nel servizio erogato è inclusa tutta la capacità elaborativa atta a supportare la replica dei workload, realizzata su due Availability Zone (AZ) geograficamente separate. In caso di fault di una Availability Zone, il servizio impattato sarà ripristinato su un'altra AZ facente parte della Region Italiana.

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

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

5.2.4 Specifiche di collaudo

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

5.3 CONSOLE UNICA

La Fornitura prevede l'erogazione alle PAC, in maniera continuativa e sistematica, di una serie di servizi afferenti ad un Catalogo predefinito e gestito attraverso una Console Unica dedicata.
Il PSN metterà a disposizione delle Amministrazioni Contraenti una piattaforma di gestione degli ambienti cloud unica (CU) personalizzata, interoperabile attraverso API programmabili che rappresenterà per la PA l'interfaccia unica di accesso a tutte le risorse acquistate nell'ambito della convenzione. In particolare, la CU garantirà la possibilità alle Amministrazioni di configurare ed istanziare, in autonomia e con tempestività, le risorse contrattualizzate per ciascuna categoria di servizio e, accedendo alle specifiche funzionalità della console potrà gestire, monitorare ed utilizzare i servizi acquisiti.
Infine, attraverso la CU, l'Amministrazione avrà la possibilità di segnalare anomalie sui servizi contrattualizzati tramite l'apertura guidata di un ticket per la cui risoluzione il PSN si avvarrà del supporto di secondo livello di specialisti di prodotto/tecnologia.

5.3.1 Overview delle caratteristiche funzionali

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

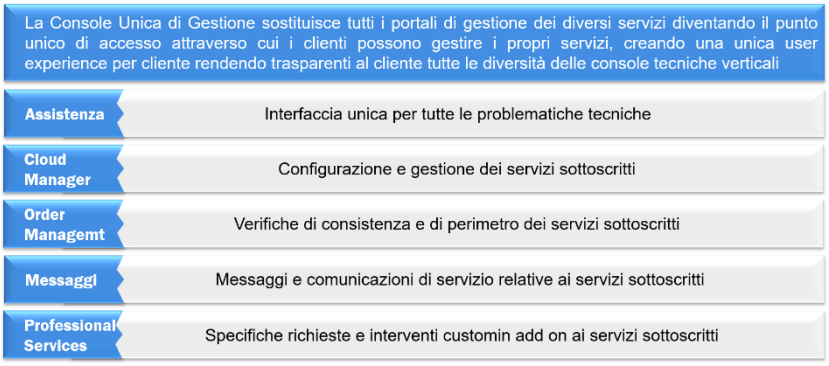


Figura 1 Funzionalità CU

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

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

dedicato alla PA, che rappresenta l'ambiente cloud tramite il quale la PA usufruirà dei servizi acquisiti (IaaS, PaaS, ecc.).

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

5.3.2 Modalità di accesso

L'accesso in modalità sicura alla Console Unica prevede l'utilizzo del sistema di Identity Management, il cui form di login è integrato nell'interfaccia web. Tale sistema gestisce le identità degli utenti registrati e consente sia l'accesso in modalità desktop, sia tramite dispositivi mobili Android o iOS. Gli utenti, autorizzati dal sistema di Identity Access Management, potranno

accedere dalla console alle risorse allocate all'interno del proprio tenant, sia per attività di "Design & Delivery" sia per attività di "Management & Monitoring".

5.3.3 Interfaccia applicativa della Console Unica

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

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

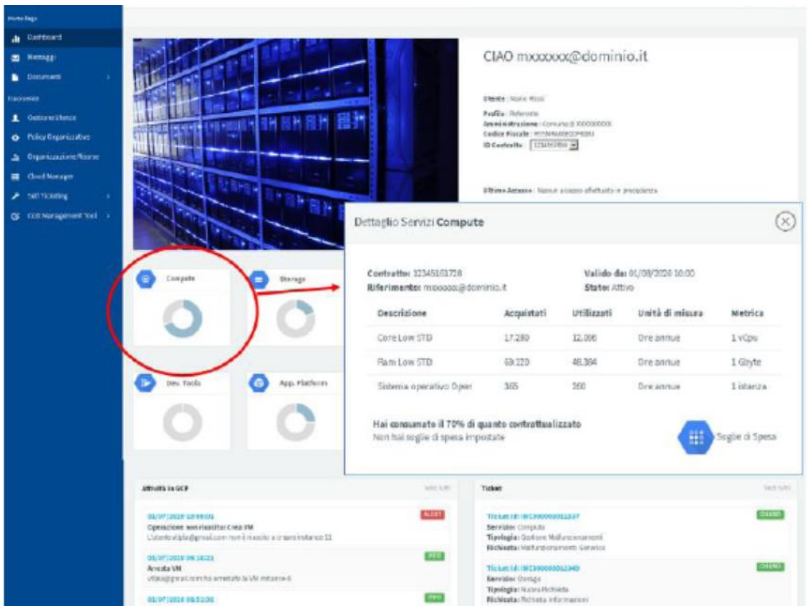


Figura 2 Dashboard CU

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

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

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

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

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

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

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

5.4 SERVIZI PROFESSIONALI

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

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

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

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

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

5.4.1 IT infrastructure service operations

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

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

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

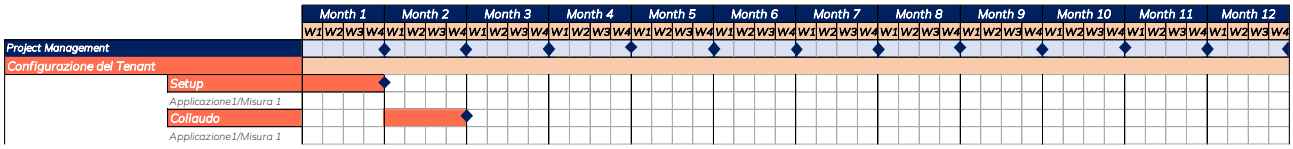
- *creazione/gestione delle utenze, dei privilegi e gli accessi ai sistemi;*
- *controllare il corretto funzionamento del Sistema Operativo, verificando i processi/servizi tramite agent di monitoring.*
- *gestione dei log di sistema e verifica delle eventuali irregolarità.*
- *gestione dei files di configurazione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

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

5.4.1.1 Personalizzazione del servizio

Come richiesto dal Piano dei Fabbisogni le attività di IT Operation sono volte alla realizzazione dell'infrastruttura Azure in grado di ospitare in una fase successiva dei servizi specifici che verranno migrati all'interno dello spazio dedicato. Tali attività verranno eseguite nella prima fase progettuale in modo tale da poter mettere a disposizione l'architettura che successivamente verrà utilizzata da servizi specifici che produrranno il consumo stimato e pattuito nel presente progetto e riportato nel configuratore a capitolo 8.

Una vista preliminare delle tempistiche delle attività può essere sintetizzata come segue:



6 FIGURE PROFESSIONALI

PSN rende disponibili risorse professionali in grado di poter supportare l'Amministrazione nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-architect, re-platform), proseguendo nella fase di riavvio degli applicativi, regression test e terminando nel supporto all'esercizio.
Per ogni progetto viene individuato il mix di figure professionali necessarie, tra quelle messe a disposizione del PSN, che effettuerà le attività richieste. Si rimanda al par. 8 Configuratore per il dettaglio dell'effettivo impegno delle risorse professionali previste per tale progetto. Il team reso disponibile per questo progetto è composto dalle seguenti figure professionali, i cui profili sono di seguito descritti:

- *Project Manager: definisce e gestisce i progetti, adottando e promuovendo metodologie agili; è responsabile del raggiungimento dei risultati, conformi agli standard di qualità, sicurezza e sostenibilità, in coerenza con gli obiettivi, le performance, i costi ed i tempi definiti.*
- *Cloud Security Specialist: esperto nella progettazione di architetture di sicurezza per sistemi basati su cloud (public ed hybrid). È responsabile per il supporto alla realizzazione delle architetture di sicurezza dei nuovi workload delle Amministrazioni e alle attività di migrazione, fornisce indicazioni e raccomandazioni strategiche ai team operativi e di sviluppo per affrontare i punti deboli della sicurezza e identificare potenziali nuove soluzioni di sicurezza negli ambienti cloud*
- *Database Specialist and Administrator: È responsabile dell'installazione, dell'aggiornamento, della migrazione e della manutenzione del DBMS; si occupa di strutturare e regolamentare l'accesso ai DB, monitorarne l'utilizzo, ottimizzarne le prestazioni e progettare strategie di backup*
- *System Architect: ha consolidata esperienza in technical/service management e project management, analizza i sistemi esistenti e definisce come devono essere coerentemente integrate le nuove soluzioni; è responsabile della progettazione della soluzione infrastrutturale e del coordinamento di specifici stream di progetto*
- *Product/Network/Technical Specialist: È responsabile delle attività inerenti all'integrazione delle soluzioni tecniche ed il supporto specialistico di prodotto nell'ambito dell'intervento progettuale.*
- *System and Network Administrator: ha competenze sui sistemi operativi, framework di containerizzazione, tecnologie di virtualizzazione, orchestratori e sistemi di configuration e versioning; è responsabile della implementazione di sistemi di virtualizzazione, di container utilizzando anche sistemi di orchestrazione e della manutenzione, della configurazione e del funzionamento dei sistemi informatici di base.*

7 SICUREZZA

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

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

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

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

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

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

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

8 CONFIGURATORE

Di seguito, l'export del Configuratore contenente tutti i servizi della soluzione con la relativa sintesi economica in termini di canone annuo e UT. La durata contrattuale (prevista per un massimo di 10 anni) dei servizi contenuti nel presente progetto sarà declinata all'interno del contratto di utenza.
I valori relativi alla infrastruttura poiché essa è erogata in modalità a consumo, sono da considerarsi dei massimali, ottimizzabili sulla base dell'effettivo utilizzo delle risorse elaborative. Il valore complessivo contrattuale è da intendersi comprensivo dei lotti opzionali. Nello specifico, il contratto base prevede gli importi indicati per il primo anno contrattuale, i due anni successivi di consumo sono da intendersi come due lotti opzionali del valore indicato.

Di seguito si riporta la stampa completa del configuratore; limitatamente alla componente infrastrutturale il canone annuale è riferito al valore a regime, ovvero considerando la disponibilità operativa degli ambienti migrati mentre i valori dei servizi professionali sono riferiti all'intera durata contrattuale.

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	80248290589
Ragione Sociale	Ministero della Difesa - Stato Maggiore della Difesa (VI Reparto)
IDENTIFICATIVO DOCUMENTO	
Emesso da	PSN M&S/CS
Codice Documento	2025-000008024829058 9-PdF-P2R1
Versione	1

RIEPILOGO PREZZI		
SERVIZIO	TOTALE UT	TOTALE CANONE ANNUALE
HybridCloudonPSNsite		€0,00
IndustryStandard	€0,00	€0,00
PublicCloudPSNManaged		€0,00
SecurePublicCloud		€1.700.232,77
ServiziMigrazione	€0,00	
ServiziProfessionali	€98.353,40	
TOTALE	€98.353,40	€1.700.232,77

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITÀ	DR	TOTALE UT	TOTALE CANONE ANNUALE
		SecurePublicCloudAzure	Compute a consumo					€1.084.149,91
	SP05	ServiziProfessionali	Figura professionale	Cloud Security Specialist	12		€3.106,56	
	SP02	ServiziProfessionali	Figura professionale	Database Specialist and Administrator	15		€3.883,20	
	SP24	ServiziProfessionali	Figura professionale	Product/Network/Technical Specialist	123		€42.789,24	
	SP07	ServiziProfessionali	Figura professionale	Project Manager	50		€19.304,00	
	SP12	ServiziProfessionali	Figura professionale	System and Network Administrator	72		€22.237,92	
	SP23	ServiziProfessionali	Figura professionale	Systems Architect	14		€7.032,48	
		SecurePublicCloudAzure	Intelligence - Artificial Intelligence					€130.184,21
		SecurePublicCloudAzure	Monitor - Azure Monitor					€51.509,24
		SecurePublicCloudAzure	Network - Bandwidth					€10.833,11
		SecurePublicCloudAzure	Network - Virtual Network					€22.015,43
		SecurePublicCloudAzure	Network - VPN Gateway					€13.746,44
		SecurePublicCloudAzure	Network Security - Azure Bastion					€12.865,78
		SecurePublicCloudAzure	Network Security - Azure Firewall					€38.515,60
		SecurePublicCloudAzure	Security Services - Azure Key Vault					€35.716,58
		SecurePublicCloudAzure	Storage					€288.098,62
		SecurePublicCloudAzure	Storage - Blob Storage					€12.597,87

9 Rendicontazione

La rendicontazione del presente progetto verrà effettuata progressivamente attraverso La consuntivazione, avverrà su base SAL mensili per la fase di migrazione e bimestrali per le fasi successive "a regime" in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali e risorse computazionali fino ad esaurimento dall'importo complessivo contrattualizzato. La fatturazione degli importi sarà effettuata sulla base dell'effettivo consumo delle risorse.

La seguente tabella rappresenta la previsione del piano di fatturazione relativa al primo anno, che comprende i servizi di "IT Infrastructure Service Operations" ed una ipotesi di fatturazione del consumo infrastrutturale al massimo dell'utilizzo.

	Peso	Importo	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Configurazione del tenant		**€ TOT**												
- Setup	**50%**	**€**	49.176,70 €											
- Collaudo	**50%**	**€**		49.176,70 €										
Consumi annui		**€ TOT**												
Canone consumo (stima del massimale a consumo)			566.744,26 €		566.744,26 €		566.744,26 €							
Totale		**€ TOT**	**615.920,96 €**	**49.176,70 €**	**566.744,26 €**	**- €**	**566.744,26 €**	**- €**	**- €**	**- €**	**- €**	**- €**	**- €**	**- €**

La stima dei consumi, che riflette i volumi ipotizzati in accordo con questa Amministrazione, potrà comunque essere oggetto di revisione nel corso dell'esecuzione delle attività, qualora se ne ravvisi la necessità.
La fatturazione sarà in ogni caso allineata agli effettivi consumi del cliente, con cadenza bimestrale posticipata.