Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 01/02/2024 09:15
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

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

CUP: J51B21005710007

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

ASL di Latina

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	31/01/2024

Tabella 1: Informazioni Documento

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

Tabella 2: Autore

Revisione:	
PSN Solution team	n.a.

Tabella 3: Revisore

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

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

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

ESTERNA A:

- Referente Contratto Esecutivo ASL di Latina Walter Battisti
  - Email: w.battisti@ausl.latina.it
- Referente Tecnico ASL di Latina Walter Battisti
  - Email: w.battisti@ausl.latina.it

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del PSN relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012.
Quanto descritto, è stato redatto in conformità alle richieste del *ASL di Latina* di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (ID 2023-0000001684950593-PdF-P1R1).

2 AMBITO

AMBITO	VALORE	DOC DI DETTAGLIO (SE DISPONIBILE)
Numero di Data Center e dislocazione sul territorio nazionale	4	
Presenza del servizio di Business Continuity	NO	
Presenza del servizio di Disaster Recovery	NO	
Quantità e tipologia di sistemi server (divisione tra sistemi fisici e sistemi dedicati alla farm virtuale)	3 Vertex DELL Biserver 5 Server DELL R640 1 Server DELL R650	Non sono presenti server fisici tutta la parte elaborativa è virtualizzata
Quantità e tipologia di Storage (SAN, NAS) (con TB presenti, occupati e disponibili)	3 Vertex storage integrato da 10TB occupato XXX 2 Compellent DELL SC5020 da 40 TB occupato 1 Unity DELL 50 TB occupato 30 TB	
Apparti SAN (quantità e caratteristiche della fabric)	4 Switch DELL modello	
Rete (quantità e caratteristiche: Bilanciatori, piano di indirizzamento, eventuali problemi nel cambio di indirizzamento IP)	N. 113 Switch	Da 10.60.0.0 a 10.60.99.255 dati; Da 10.60.112.0 a 10.60.164.255 radiologia; 172.16.0.0/16 management; 172.19.0.0/16 VoIP su MPLS 172.20.0.0. VoIP su RanSan
Sistemi di sicurezza (quantità e caratteristiche) (Identity & Access Management, Firewall, Sonde, Waf, Soc, etc.)	1 IAM RedHat Keyclock in HA integrato AD Microsoft AD 1 Firewall SonicWall in HA	
Servizio di Active Directory	5 DC	

AMBITO	VALORE	DOC DI DETTAGLIO (SE DISPONIBILE)
Sistemi di virtualizzazione (VMware, Hyper-V, RedHat)	VMware	
In caso di presenza di VMWARE specificare: N° di vCenter e versioni	5 Vcenter ver. 7	
In caso di presenza di VMWARE specificare: Presenza di prodotti NSX-T, vRNI, vROPS, HCX, etc.	No	
Sistemi fisici dedicati alla farm Vmware (Fornire RVTools)	SI	
storage fisici dedicati alla farm Vmware (Fornire RVTools)	SI	
Presenza di sistemi Iperconvergenti (vSAN, nutanix, DELL VxRAIL, tec.)	NO	
Backup, prodotti utilizzati (fornire schema topologico se disponibile, N° master e N° media server)(N° master e N° media server)	DELL Avamar	
Policy di Backup (TB sottoposti a backup e retention)		
Librerie e storage dedicati al backup	2 data domain DELL virtuali da 8TB 1 Data Domain DELL modello 3300 1 Data Domain DELL modello 6300	
Piattaforme middleware (quantità e caratteristiche), identificare applicazioni single istance	Spagic WSO2 Spagic	
Identificazione cluster di sistema operativo (Windows, RedHat, Solaris, etc.)	Windows, RedHat, Oracle Linux, Ubuntu	
Database (quantità e caratteristiche)	SI	MySql, MS SQL, Maria DB, Oracle
Sistemi di posta elettronica (PEL e PEC)	PEL Postfix, Roudcube, Dovecot	
Siti e portali (quantità e caratteristiche)	1 Sito Web Apache 1 Portale Applicativo server Payara	

AMBITO	VALORE	DOC DI DETTAGLIO (SE DISPONIBILE)
È presente una stima del capacity? (eventuale previsione di crescita) in caso affermativo fornire i dati	SI	30%
Presenza di un CMDB accurato del cliente con elenco delle applicazioni	SI	Limitatamente alla parte CLIENT
Il Data Center sorgente è gestito internamente o da fornitori terze parti?	Da fornitori esterni (SGM)	
Le applicazioni vengono gestite internamente o da fornitori terze parti?	Da fornitori esterni	
Sono disponibili strumenti di monitoraggio delle applicazioni e della rete?	Si intermapper per la rete è in fase di installazione zabbix	
Presenza e tipologia di appliance fisici	NO	
Prodotti Antivirus	Bitdefender	
Sistema di gestione delle password	Microsoft laps	
Qual è il numero totale di workloads presi in considerazione per questo progetto?	132	
Eventuali workload fisici da migrare (tipologia e quantità) (P2V)	0	
Tipologie e versioni di sistema operativo (Windows, Linux, etc.)	Windows 2016, 2019, 2022, RedHat 8, Oracle Linux 8, Ubuntu 22.04, Centos 7	
Contesto applicativo – numero di applicativi	44	
Contesto applicativo – servizi e vendor	Engineering, dedanext, dedalus, altri minori	

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Titolo	Documenti consegnati	Versione	Data versione
#1	Piano dei Fabbisogni di Servizio	PSN_Piano dei Fabbisogni_v1.0	1.0	01.12.2022
#2	Piano di Sicurezza	PSN-SDE-CONV22-001-PianoSicurezza v.1.0 Allegati: PSN - Processo IM v.03 2.C Qualificazione Servizi Cloud 2.B Fornitore Servizio Cloud 2.A Soggetto Infrastruttura Digitale	1.0	22.12.2022
#3	Piano di Qualità	PSN-SDE-CONV22-001-Piano della Qualità	1.0	22.12.2022
#4	Piano di Continuità Operativa	PSN-SDE-CONV22-001-Piano di Continuità Operativa ver.1.0	1.0	22.12.2022

Tabella 5: Documenti Contrattuali

3.2 DOCUMENTI DI RIFERIMENTO

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

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022	CONVENZIONE ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l'affidamento in concessione dei servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili - "Polo Strategico Nazionale"

Riferimento	Codice	Titolo
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
DB	DataBase
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
VM	Virtual Machine

Tabella 8: Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

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

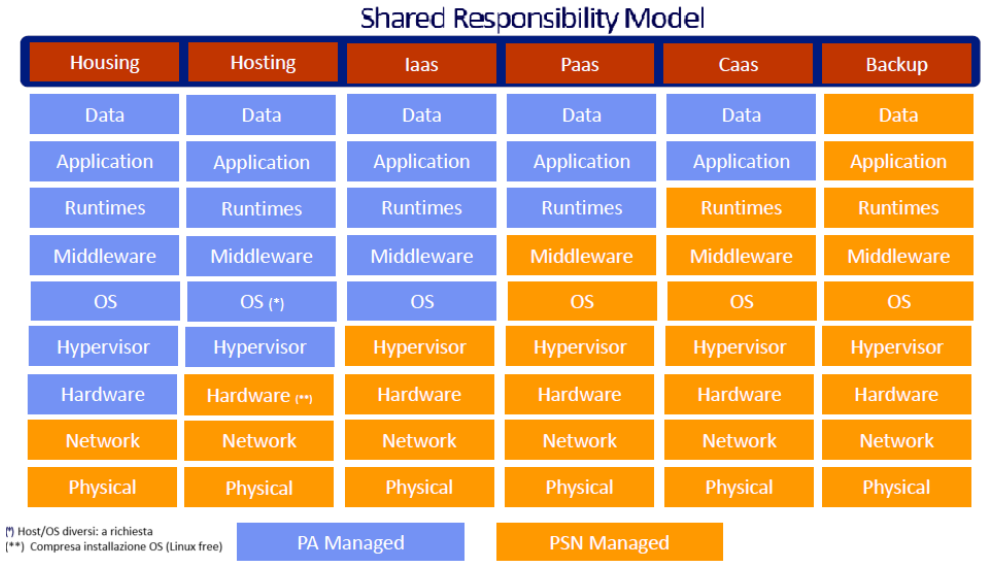
5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
Industry Standard	Housing
Industry Standard	Infrastructure as a Service (IaaS)
Industry Standard	Data Protection: Backup
Industry Standard	Data Protection: Golden Copy
Industry Standard	Container as a Service (CaaS)
Industry Standard	Connettività
Public Cloud PSN Managed	Licensed SQL eOracleHyperscalerTechnology
Servizi di Migrazione	
Servizi Professionali	Re-Architect

Tabella 9: Servizi Proposti

Di seguito, è mostrata la matrice di responsabilità nell'ambito della gestione dei servizi migrati su PSN:



Classificazione dei Dati durante la migrazione:

Wave	SERVIZIO ACN	CLASSIFICAZIONE
1	ASSISTENZA SANITARIA DI BASE	CRITICO
	EMERGENZA SANITARIA TERRITORIALE	CRITICO
	ASSISTENZA FARMACEUTICA	CRITICO
	ASSISTENZA INTEGRATIVA	CRITICO
	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO
	ASSISTENZA PROTESICA	CRITICO
	ASSISTENZA TERMALE	ORDINARIO
	ASSISTENZA SOCIOSANITARIA A MINORI, ALLE DONNE, ALLE COPPIE, ALLE FAMIGLIE	CRITICO
	ASSISTENZA RESIDENZIALE E SEMI-RESIDENZIALE	CRITICO
	PRONTO SOCCORSO	CRITICO
	RICOVERO ORDINARIO PER ACUTI	CRITICO
	DAY SURGERY	CRITICO
	DAY HOSPITAL	CRITICO
	RIABILITAZIONE E LUNGODEGENZA A POST ACUZIE	CRITICO

	ATTIVITA' TRASFUSIONALI	CRITICO
	ATTIVITA' DI TRAPIANTO DI CELLULE, ORGANI E TESSUTI	CRITICO
	ATTIVITA' DIAGNOSTICA	CRITICO
2	ASSISTENZA SPECIALISTICA AMBULATORIA	CRITICO
	SORVEGLIANZA, PREVENZIONE E CONTROLLO DELLE MALATTIE INFETTIVE E PARASSITARIE, INCLUSI I PROGRAMMI VACCINALI	CRITICO
	SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	ORDINARIO
	SORVEGLIANZA E PREVENZIONE DELLE MALATTIE CRONICHE, INCLUSI LA PROMOZIONE DI STILI DI VITA SANI ED I PROGRAMMI ORGANIZZATI DI SCREENING; SORVEGLIANZA E PREVENZIONE NUTRIZIONALE	ORDINARIO
	ASSISTENZA A PARTICOLARI CATEGORIE	CRITICO
	RETI DI PATOLOGIA	CRITICO
	RISCHIO CLINICO	CRITICO
	EDUCAZIONE CONTINUA IN MEDICINA	ORDINARIO
	ANAGRAFE NAZIONALE ASSISTIBILI	CRITICO
	FASCICOLO NAZIONALE ASSISTIBILI	CRITICO
	RAPPORTO CON L'UTENZA - URP	ORDINARIO
	COMUNICAZIONE ISTITUZIONALE WEB E OPENDATA	ORDINARIO
	PROTOCOLLO	ORDINARIO
	GESTIONE DOCUMENTALE	ORDINARIO
	CONSERVAZIONE DIGITALE	ORDINARIO
	PERSONALE	ORDINARIO
	CONTABILITA', BILANCIO E CONTROLLO	ORDINARIO
	ACQUISTI	ORDINARIO
	PRODUTTIVITA' INDIVIDUALE E COLLABORATION	ORDINARIO

5.2 INDUSTRY STANDARD

5.2.1 Housing

5.2.1.1 Descrizione del servizio

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

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

Tipologia	Elemento	Caratteristiche tecniche minime	Quantità	Durata (mesi)
Housing	IP Pubblici /29 (8 indirizzi)		4	120

Tabella 10: Fabbisogno Housing

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

5.2.1.3 Specifiche di collaudo

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

5.2.2 Infrastructure as a Service

5.2.2.1 Descrizione del servizio

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

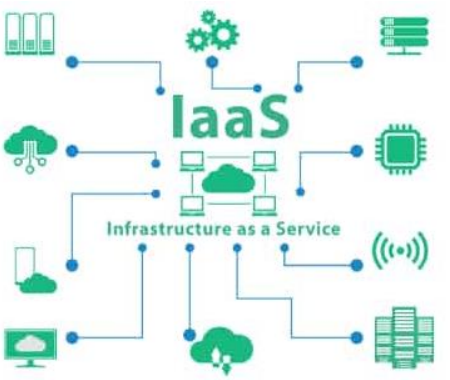


Figura 1 Infrastructure as a Service

Il servizio IaaS è suddiviso in:

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

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

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

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

5.2.2.2 Personalizzazione del servizio

L'obiettivo, quindi, è di massimizzare la qualità del servizio offerto ottenendo:

- Riduzione dei tempi di risposta
- Rispetto dei Service Level Objectives
- Attivare sistemi di proattività nella gestione degli incidenti

Per questi motivi l'amministrazione ha scelto la soluzione IaaS Private.

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

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
IaaS Private (HA)	Blade Large	36	768				Server features 2 socket Intel® Xeon® Scalable processor family, with up to 32 DIMMs (up to 6TB), PCIExpress® (PCIe) 4.0 enabled I/O slots, and 2 high bandwidth Ethernet and Fiber Channel mezzanine card. All Ethernet interfaces are 10/25Gbps, fully redundant, with jumbo frame enabled end to end in the overall infrastructure. All FC interfaces are 32Gbps. Processore Intel 6354, 18 core, 3.0GHz, cache 39MB, 205W. Sistema operativo escluso	6	120
IaaS - Storage (HA)	Storage High Performance					500	SAN NVMe based, replicato intra-region, 170K IOPS per Storage Array	100	120
IaaS - Storage (HA)	Storage HP Encrypted					500	SAN NVMe based, replicato intra-region, crittografato a livello di singolo volume, 170K IOPS per Storage Array	40	120

Tabella 11: Fabbisogno IaaS

Si conferma che i dati critici saranno conservati sullo storage di tipo Encrypted.

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

5.2.2.4 Specifiche di collaudo

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

5.2.3 Data Protection e Disaster Recovery

5.2.3.1 Data Protection: Backup

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

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

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

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

5.2.3.2 Data Protection: Golden copy protetta

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

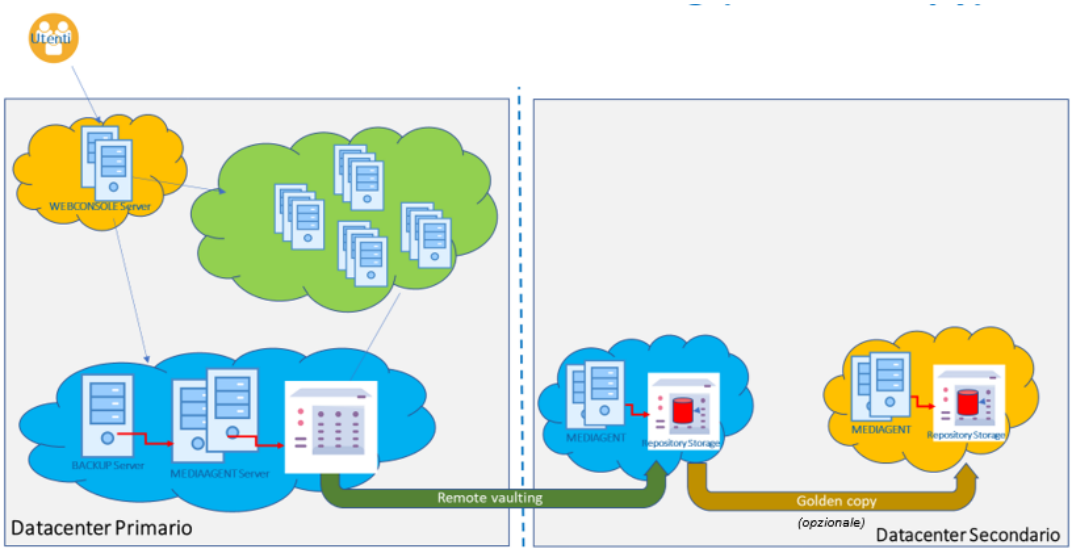


Figura 2 Architettura Funzionale Golden Copy

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

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

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

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)

Data Protection	Backup					1.000	Gestione delle policy in modalità self-managed; cifratura dei dati; ripristino granulare dei dati in modalità "a caldo e out-of-place"; seconda copia intra-region; GDPR compliant	105	120
Data Protection	Golden copy					1.000	Protezione antivirus, antimalware e anti-ramsonware proattivo; WORM copy; archiviazione in ambiente protetto privo di ogni accesso fisico e logico	105	120

Tabella 12: Fabbisogno Data Protection

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

5.2.3.4 Personalizzazione del servizio

Sono previste le seguenti policy: 1 full, 10 incrementali, 5% di tasso variazione dati, quota parte Golden Copy 100%.

5.2.3.5 Specifiche di collaudo

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

5.2.4 Container as a Service

5.2.4.1 Descrizione del servizio

Il Servizio Infrastrutturale in modalità Container as a Service (CaaS) consiste nella messa a disposizione, da parte del PSN, di una infrastruttura in grado di distribuire e gestire tutte le applicazioni basate su container in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica descritti nel § 3. *Sicurezza* e § 4. I*nfrastruttura e Network* del documento "Progetto di Fattibilità".
La piattaforma CaaS è realizzata in tecnologia VMware (TANZU) e in tecnologia OpenSource in funzione della tipologia eventualmente già implementata dalla PA, oppure in funzione delle sue preferenze. Si tratta comunque di due soluzioni basate su Kubernetes e quindi in grado di abilitare una logica multi-cloud (i Container basati su Kubernetes possono essere «spostati» sui Cloud Pubblici in modo semplice.

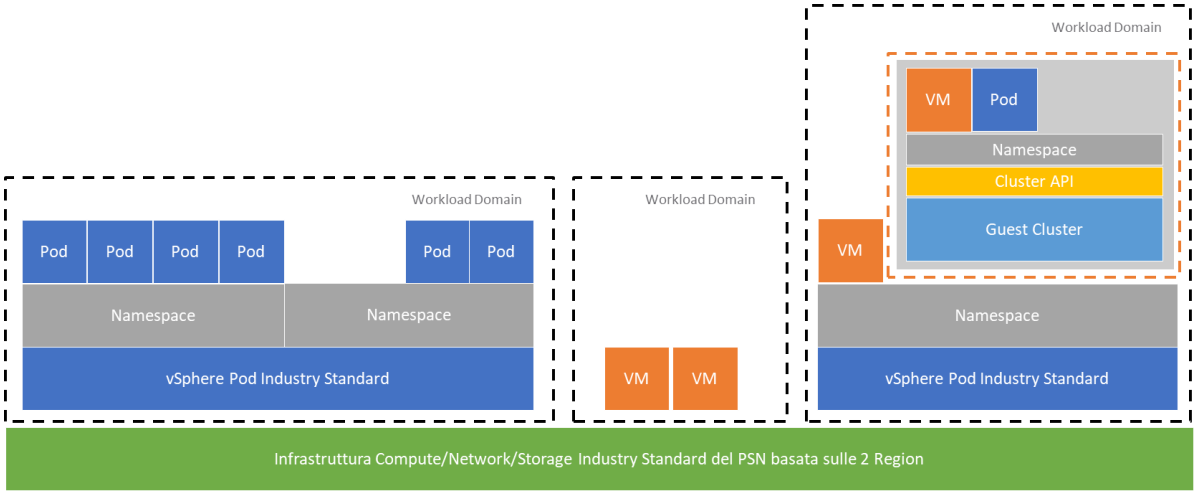


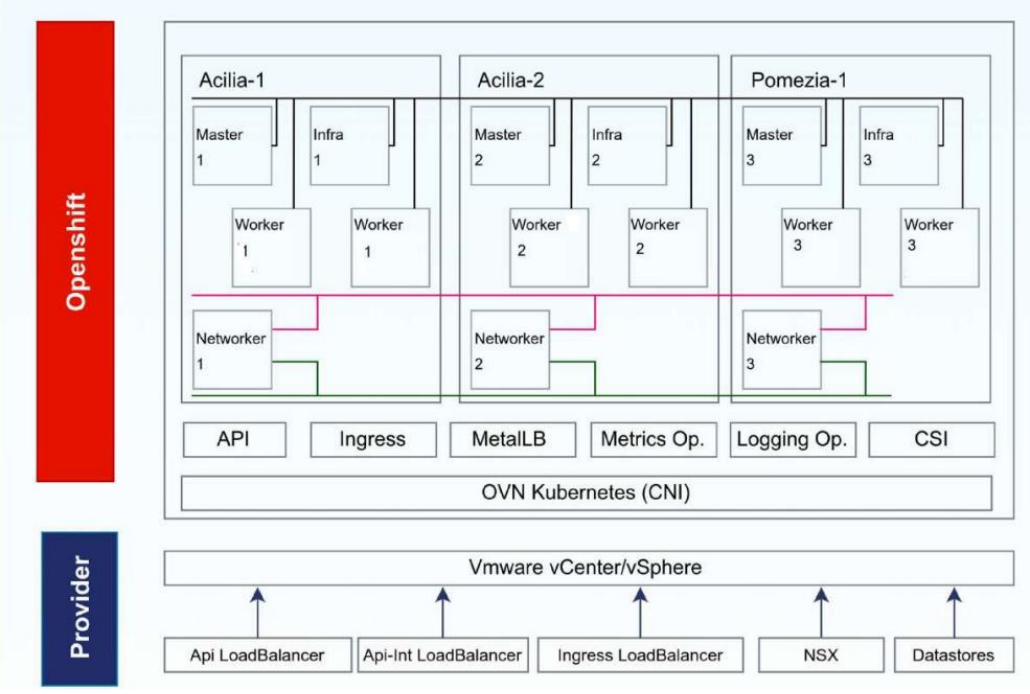
Figura 3 Container as a Service

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

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
CaaS	Open Source (vCPU/anno) Creare su AZ 1						Gestione ambienti kubernetes based	72	120
IaaSSharedHA	Pool 1GB ram aggiuntivo							288	120

Tabella 13: Fabbisogno CaaS

L'infrastruttura PSN prevede una ridondanza su tre AZ. Il dimensionamento delle risorse del servizio CaaS Opensource è stato dimensionato al fine di garantire il fault di una zona e la distribuzione del worker sulle restanti.



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

5.2.4.3 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 PUBLIC CLOUD PSN MANAGED

5.3.1 Descrizione del servizio

Il Public Cloud PSN Managed è un servizio PSN Core che permette alle PA di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica degli ambienti e gestione operata da personale PSN.
Relativamente al modello di servizio Public Cloud PSN Managed, nella prima figura che segue vengono messe in risalto le differenze e integrazioni con il modello Public Cloud puro in Region Italiana; nella seconda se ne descrivono l’architettura e l’interconnessione.

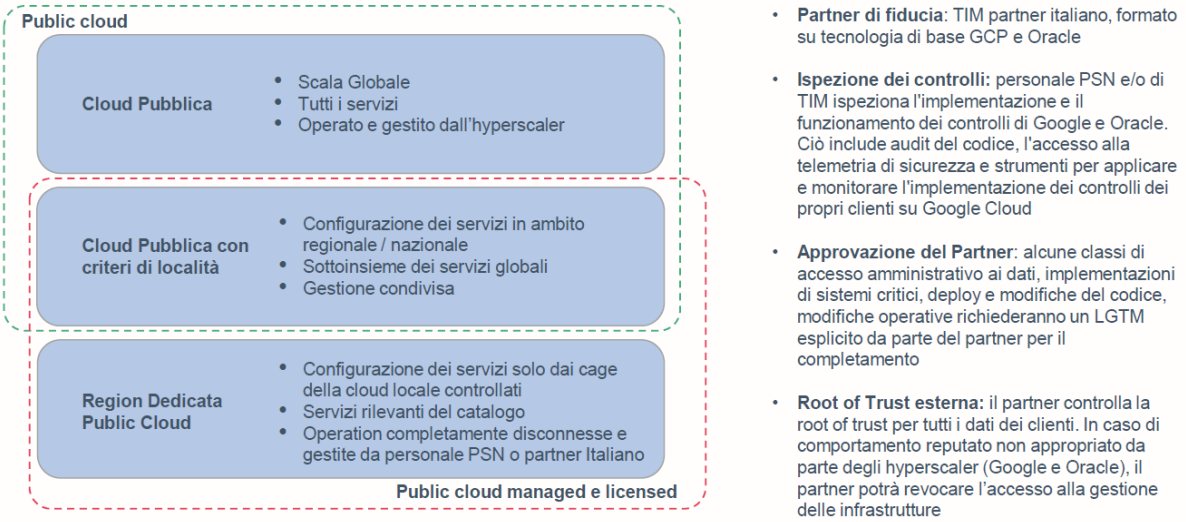


Figura 4 Public Cloud vs Public Cloud Managed

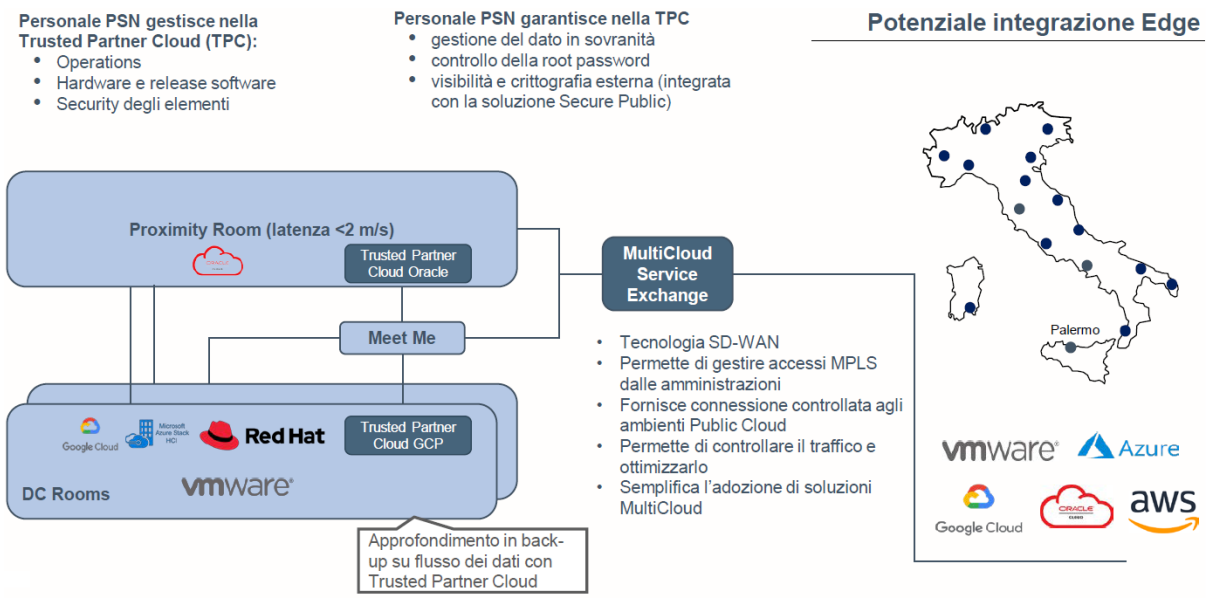


Figura 5 Architettura Public Cloud Managed

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

GCP (Google Cloud Platform)

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

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

Oracle Cloud

Per quanto concerne Oracle, la soluzione nativa è realizzata sul modello di Oracle Region Dedicated. L'architettura prevede una modularità in grado di sfruttare sia singoli componenti tecnologici dedicati (es. x86 systems, Exadata appliance, ecc), sia l'intera Region, in contiguità con la Region Google.

La gestione di tali servizi include in particolare le seguenti aree di attività:

- Segregazione Sicurezza di Rete;
- Segregazione livello dati;
- Gestione dei rilasci del Software Oracle Cloud;
- Implementazione della Gestione dei Costi e dei consumi;

- Gestione, sostituzione e dismissione dei componenti hardware dell'infrastruttura sottesa dai servizi, in modalità Escorted con personale Oracle e TIM.

Il servizio

Il Public Cloud PSN Managed realizza un modello di servizio del tutto analogo al Public Cloud del CSP (o Hyperscaler), ma rispetto ad esso permette di implementare una logica di separazione logica e fisica, sia nella gestione operativa che nel rilascio e controllo del software di base che caratterizza il servizio.

La Region dedicata permette al personale del PSN di esercitare direttamente il controllo sui servizi del CSP, a tutti i livelli di esecuzione, per l'erogazione dei servizi dedicati alle PA:

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

Il PSN dispone di istanze del cloud Hyperscaler aggiungendo i propri domini, indirizzi IP, branding, fatturazione ed è integrato con servizi di Crittografia del PSN stesso. Queste istanze possono essere totalmente disconnesse nel caso sorga la necessità di tutelare la sicurezza nazionale.

Tale Region dedicata può essere usata per i massimi livelli di confidenzialità dei dati grazie alla sua implementazione dedicata al PSN, garantendo però allo stesso tempo tutti i vantaggi di un cloud Hyperscaler quali ad esempio elasticità, completezza di servizi, innovazione e scalabilità.

Gli attori coinvolti nella realizzazione del servizio Public Cloud PSN Managed sono:

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

L'MSP-PSN è responsabile end-to-end della gestione operativa della Region dedicata; ha accesso esclusivo ai sistemi per l'hosting dei servizi cloud e se necessario potrà avvalersi della consulenza del CSP nella risoluzione degli Incident.

Le attività svolte dall'MSP-PSN includono la progettazione, l'attivazione, la gestione e il controllo dei servizi cloud, come:

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

Architettura fisica

Il Public Cloud PSN Managed è implementato all'interno di una delle Region dedicata al PSN, prevedendo la possibilità di fornire un disaster recovery in un'ulteriore Region collocata fisicamente ad almeno 100Km di distanza dalla principale per garantire resilienza in caso di eventi di disastro.

Nelle zone il CSP individuerà delle aree per isolare fisicamente gli apparati dedicati al PSN, e l'MSP-PSN avrà in carico il totale controllo degli accessi a tali aree (se necessario anche inibendo del tutto l'accesso al CSP). In caso di necessità il personale del CSP potrà accedere (ad esempio per fare degli interventi on-site), ma dovrà essere sempre accompagnato da un responsabile dell'MSP-PSN (accesso escorted).
Sarà possibile per l'MSP-PSN anche ispezionare gli strumenti e le apparecchiature usate per gli interventi.
Ripartizione delle responsabilità
Il modello Public Cloud PSN Managed prevede una ripartizione delle responsabilità che lascia all'MSP-PSN il pieno controllo dei layer che vanno dalla gestione logica della rete fino alla sicurezza applicativa.
Il CSP ha la responsabilità di gestire il provisioning dell'HW e degli altri asset fisici e di fornire la piattaforma software per la gestione e l'implementazione dei servizi, lasciando comunque all'MSP-PSN la possibilità di fare code inspections e la review delle modifiche.
Controllo della Rete
L'MSP-PSN ha piena autonomia e totale controllo del traffico di rete da e verso il PSN. Il controllo prevede la possibilità di ispezionare, loggare e bloccare tutto il traffico, mediante dei control proxy scelti da vendor certificati (e non necessariamente forniti dal CSP). Il controllo del traffico riguarda sia i dati (payload) che il traffico per il controllo e l'amministrazione. Tutto ciò a garanzia della totale copertura del rischio di data extrafiltration e di accessi non autorizzati ai sistemi.
Accesso verso l'esterno Frontend
L'MSP-PSN fornisce, gestisce e controlla tutti gli accessi alla rete pubblica: Blocchi di indirizzi IP, peering con le reti di altri providers, ecc.
Se richiesto l'MSP-PSN potrà disporre anche di propri DNS, load balancer, VIP tunneling e strumenti di gestione aggiuntivi.
Rientra inoltre sotto il controllo dell'MSP-PSN anche tutta la gestione delle key chains: nomi di dominio, certificati TLS, CA, rotazione delle chiavi, scadenza, ecc.
Encryption at-rest
Tutti i dati verranno cifrati in modo trasparente at-rested in-transit. Le chiavi di cifratura saranno custodite dall'MSP-PSN su apparati certificati (HSM) di sua proprietà e collocati fisicamente all'esterno del perimetro controllato dal CSP. L'accesso alle chiavi custodite nell'HSM dell'MSP-PSN sarà sempre soggetto ad approvazione ed audit (sia nel caso di accesso consentito, sia nel caso di accesso negato). L'auditing dovrà avvenire su dei sistemi di persistenza che escludano il rischio di manomissione dei log (sia cancellazione che modifica). Il CSP in nessun modo avrà accesso fisico o disponibilità di utenze con privilegi di accesso all'HSM. Tutti i dati (inclusi i backup) custoditi all'interno del Public Cloud PSN Managed saranno cifrati con questo meccanismo. Sarà cura dell'MSP-PSN custodire le chiavi garantendo l'alta disponibilità e la protezione da eventuali eventi di disastro, per scongiurare l'impossibilità di poter decifrare i dati.
Gestione degli Aggiornamenti
Tutti i CSP prevedono degli aggiornamenti frequenti sia ai servizi che ai sistemi di gestione (Continouos deployment) per rilasciare fix, nuove features o rimedi ad esposizioni di sicurezza: uno dei vantaggi del Public Cloud PSN Managed consiste proprio nel poter sfruttare questi benefici (soprattutto la celerità nel rimediare a potenziali esposizioni di sicurezza). Allo stesso tempo però l'MSP-PSN deve tutelare il PSN da eventuali modifiche che in modo malevolo (anche senza la consapevolezza del CSP) possano mettere a rischio la sicurezza delle applicazioni o dei dati.

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

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

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

Tipo	Tipologia	Tipo	Unit	Time	Quantità	Durata mesi
Licensed SQL e Oracle Hyperscaler Technology	SQL instances	Gen 2 Exadata Cloud at Customer - Database OCPU - BYOL	OCPU	hour	20	120

Tabella 14: Fabbisogno PublicCloudPSNManaged

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

5.3.3 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.

5.4 Connettività

5.4.1 Descrizione del servizio

Si provvederà a realizzare un collegamento MPLS (master) presso la sede principale della ASL di Latina e uno (slave) presso il DC PSN ad uso migrazione.

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

Tipologia	Elemento	CORE [Q]	RAM [GB]	vCPU [Q]	vRAM [GB]	Storage [GB]	Caratteristiche tecniche minime	Quantità	Durata (mesi)
Connettività	Connessione dedicata 1 Gbps						Tecnologia Gbe MPLS, profilo Silver 1000, TIR L2/L3 e outsourcing	2	12

Tabella 15: Fabbisogno Connettività

La connettività MPLS sarà utilizzata soltanto per la durata della migrazione. Al termine di essa il servizio verrà cessato.

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

5.4.3 Specidfiche 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.

5.5 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.

5.5.1 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".

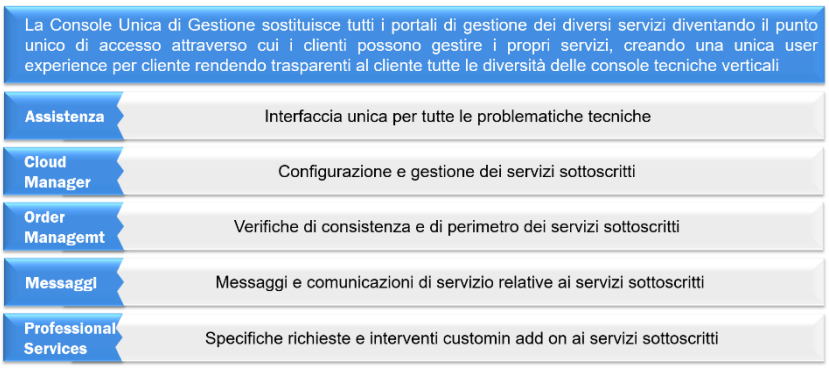


Figura 6 Funzionalità CU

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.).

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

5.5.2 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".

5.5.3 *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.).

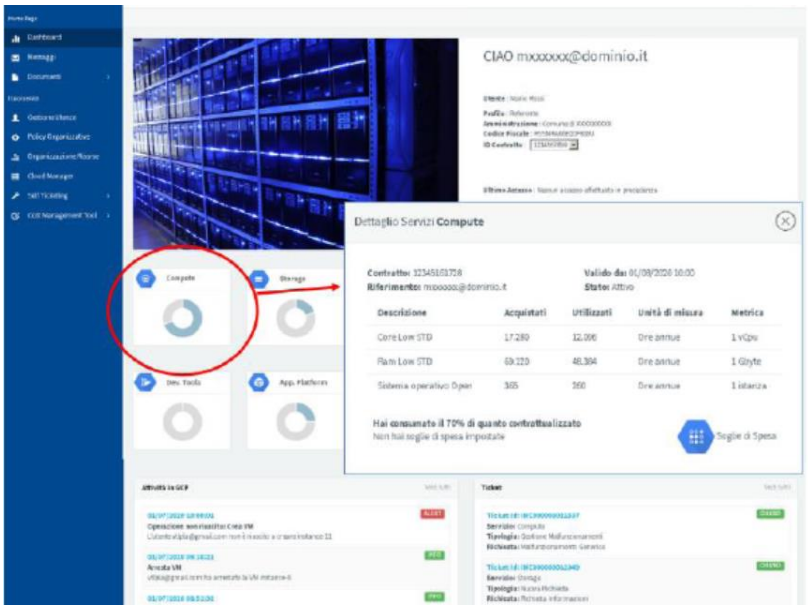


Figura 7 Dashboard CU

- 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.

5.6 SERVIZI E PIANO DI MIGRAZIONE

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assessment effettuati in fase di definizione delle esigenze dell'Amministrazione, tenendo conto di eventuali vincoli temporali ed architetturali di dettaglio oltre che di specifiche esigenze di customizzazione.

Per l'intero periodo di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

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

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

Verranno inoltre condivisi:

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

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

- Explore, che include le fasi relative all'analisi e alla valutazione dell'ambiente, per aiutare la PA a definire il proprio percorso di migrazione verso il cloud.

- Make, che comprende tutte le attività di design e di predisposizione dell'ambiente per permettere la migrazione in condizioni di sicurezza, tra cui anche i test necessari a validare il disegno di progetto.
- Go, che prevede il collaudo, l'attivazione dei servizi sulla nuova infrastruttura ed anche le attività di post go live necessarie al supporto e all'ottimizzazione dei servizi nel nuovo ambiente.

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

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

Figura 8: Servizio di Migrazione - Metodologia EMG2C

1. Analisi e Discovery

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

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

In particolare questa fase di occuperà di reperire le informazioni:

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

i) Energy Optimization.

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

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

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

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

2. Set-up

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

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

3. Migrazione

Tale fase si articola nei seguenti step:

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

4. Collaudo

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

Esecuzione Collaudo Infrastrutturale: tale fase consiste nell'esecuzione dei test dei servizi PSN attivati e definiti in precedenza con la PA per poter poi procedere con il collaudo Applicativo.

Esecuzione Collaudo Applicativo: tale fase consiste nell'esecuzione dei test per certificare il Go Live delle applicazioni su ambiente target.

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

5.6.1 Descrizione della migrazione

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

ASL Latina richiede i servizi infrastrutturali e sistemistici di migrazione strettamente necessari alla stessa secondo il piano e i requisiti definiti ai capitoli precedenti. L'Azienda necessita di concludere la migrazione entro i tempi stabiliti e nei limiti dei vincoli tecnologici e delle esigenze espresse, coinvolgendo all'interno del progetto tutti i vendor software necessari per la migrazione di tutto il parco applicativo in scope, secondo quanto meglio espresso nel seguito del paragrafo.

In particolare, l'Azienda necessita di due tipologie di servizi di migrazione:

- Servizi per la migrazione applicativa
- Servizi infrastrutturali propedeutici alla migrazione

<u>Servizi per la migrazione applicativa</u>

I Servizi per la migrazione applicativa si riferiscono a tutte le attività volte al corretto moving delle applicazioni dall'attuale infrastruttura al Polo Strategico Nazionale, che si rendono necessari in base alla modalità di migrazione lift & shift ipotizzata da ASL Latina.

I Servizi per la migrazione applicativa includono ad esempio:

- La Re-installazione dell'intera applicazione ove necessario;
- La Re-installazione di alcuni moduli ove necessario;
- L'Aggiornamento dell'applicazione ove necessario;
- La riconfigurazione dell'applicazione a valle della migrazione ove necessario;
- I Test post-migrazione;
- Altre attività in ambito applicativo.

<u>Servizi infrastrutturali propedeutici alla migrazione</u>

Tali servizi si rendono necessari in aggiunta a quelli applicativi al fine di analizzare, progettare, effettuare e governare la migrazione. In particolare, a titolo esemplificativo e non esaustivo, si riportano di seguito alcune delle attività in capo al/ai fornitore/i di servizi infrastrutturali di migrazione:

- Effettuare l'assessment e la discovery completa dell'ambiente e dei sistemi di partenza al fine di progettare la migrazione;
- Progettare la rete e più in generale la landing zone;
- Predisporre la landing zone;
- Effettuare il set up delle risorse atte alla migrazione;
- Definire le corrette modalità di utilizzo dei tool messi a disposizione dal PSN;

- Effettuare tutte le attività sistemistiche per la reinstallazione, riconfigurazione o Migrazione L&S delle VM, dei Middleware e di tutto lo stack software atto al running delle applicazioni;
- Effettuare altre attività infrastrutturali e sistemistiche in linea con i fabbisogni;
- Migrare le Virtual Machine di ASL Latina in modalità L&S: i fornitori infrastrutturali devono garantire un supporto completo dal punto di vista dell'infrastruttura ai fornitori di software durante il processo di migrazione delle macchine virtuali. Non si hanno requisiti specifici riguardo alla responsabilità dell'attività di moving delle VM/import-export; tuttavia, in assenza di un fornitore di software, è compito del fornitore dell'infrastruttura effettuare tale operazione. In altre parole, questa responsabilità ricade sui fornitori di infrastruttura nel caso in cui non sia presente un fornitore software di riferimento per uno specifico server.
- Garantire la gestione delle attività tecniche di migrazione e quindi il governo centrale degli attori tecnici coinvolti, al fine di pianificare le attività tecniche e assicurare un'esecuzione nel rispetto del piano stesso.

Le giornate previste per i servizi di migrazione sono riportate nella seguente tabella:

Figura	Q.tà
Cloud Application Architect	299
Database Specialist and Administrator	186
System Integrator & Testing Specialist	130
Cloud Application Specialist	283
Cloud Security Specialist	332
Enterprise Architect	279
Project Manager	739
Business Analyst	200
DevOps Expert	120
System and Network Administrator	155
Security Principal	150
Systems Architect	211
Product/Network/Technical Specialist	242

5.6.2 Piano di attivazione e Gantt

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

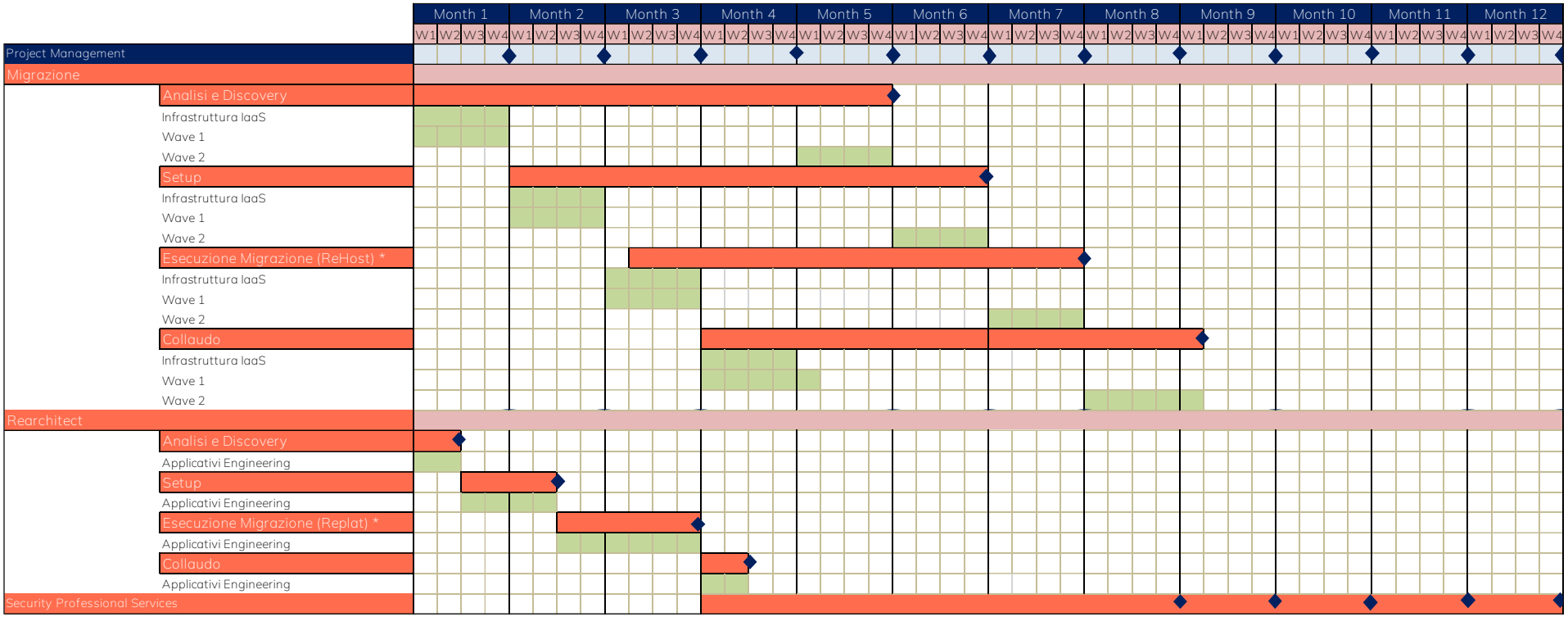


Tabella 16: Ipotesi Gantt

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

5.7 SERVIZI PROFESSIONALI

5.7.1 Re-architect

La strategia di Re-architect ha come obiettivo quello di adattare l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare i servizi cloud-native offerti dal PSN per massimizzare i benefici che ne derivano. L'obiettivo è garantire i benefici attesi dall'Amministrazione e il minimo impatto per gli utenti finali. Il servizio si rende necessario, ad esempio, quando il livello di sicurezza è molto distante dallo standard minimo e realizza la modifica di moduli applicativi di un'applicazione al fine di garantirne un adeguato livello di sicurezza

Il servizio sarà disegnato rispettando i principi di design cloud-native che non solo consente di favorire la flessibilità operativa dei servizi applicativi, ma consente anche:

- un maggior riuso e velocità di implementazione
- l'utilizzo di metodologie consolidate di test (quanto più automatici) sia per le verifiche funzionali, sia per quelle di qualità e sicurezza
- l'uso di best practices di sviluppo e di progettazione (definite dal PSN) che consenta la trasformazione del codice applicativo in modo controllato
- una progettazione secondo le metodologie Secure by design

Discorso analogo vale per il monitoraggio delle applicazioni a valle di un progetto di "re-architect". L'adozione matura di metodologie cloud-native permette all'applicazione di usufruire di piattaforme comuni di monitoraggio e manutenzione proattiva.

Di seguito vengono illustrati i diversi step del processo di Re-architect.

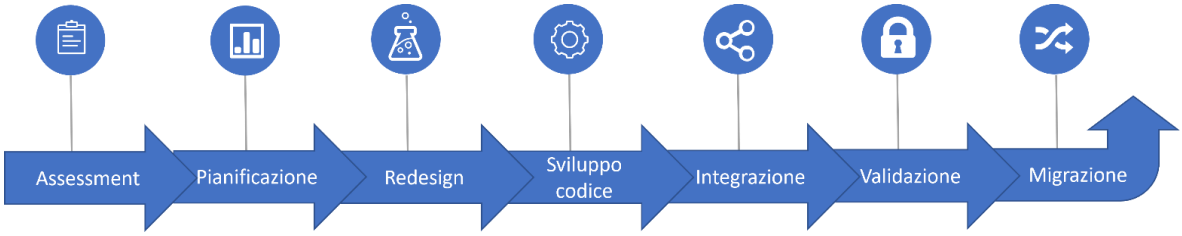


Figura 9: Flusso processo di Re-architect

Tra le attività svolte in un processo di re-architect vi è l'esecuzione dei test dei servizi PSN attivati e definiti in precedenza per certificare il Go Live delle applicazioni su ambiente target da un punto di vista infrastrutturale.

Polo Strategico Nazionale garantisce che, rispetto alle componenti applicative in ambito oggetto di re-architect, verranno identificate, documentate e risolte eventuali vulnerabilità di sicurezza in coerenza con le linee guida e misure tecniche/organizzative relative allo sviluppo sicuro del software adottato da PSN e dalla PA.

La garanzia di risoluzione delle predette vulnerabilità verrà accertata e comunicata al cliente attraverso l'esecuzione di un'attività di verifica (ad es. penetration test e vulnerability assessment) eseguita prima della messa in esercizio delle componenti oggetto dei servizi di re-architect, nel rispetto delle tempistiche concordate.

Le giornate previste per i servizi di Rearchitect sono riportate nella seguente tabella:

Figura	Giornate
Project Manager	13
Product/Network/Technical Specialist	263
Cloud Application Specialist	27
Systems Architect	25

5.7.1.1 Personalizzazione del servizio

Oggetto del rearchitect è l'ambito applicativo Openlis con l'esigenza di accorpamento dei 4 DB attualmente in esercizio in un solo DB complessivo, con la necessaria rivisitazione architetturale delle componenti di stampa etichette e di tutte le componenti di interconnessione applicativa.

5.7.2 Security Profess. Services

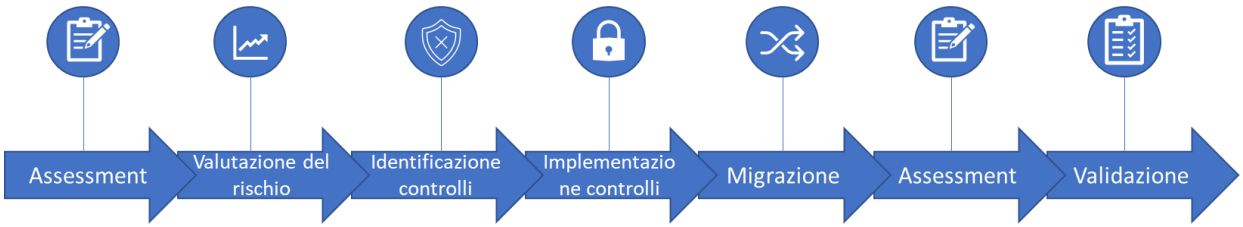
La migrazione su cloud è un processo complesso e un cambiamento rilevante che non va preso alla leggera. Non esiste una procedura di migrazione immediata sul cloud, e anzi spesso i rischi di migrazione stessi non vengono opportunamente valutati con il risultato che un'attività di migrazione che dovrebbe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

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

I servizi sono necessari per:

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

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



Le giornate previste per i servizi di Sicurezza sono riportate nella seguente tabella:

Figura	Giornate
Cloud Application Architect	443
Cloud Application Specialist	708
Data Protection Specialist	620
Forensic Expert	354
Junior Information Security Consultant	708
Junior Penetration Tester	531
Junior Security Analyst	885
Project Manager	531
Security Principal	443
Security Solution Architect	885
Senior Information Security Consultant	443
Senior Penetration Tester	354
Senior Security Auditor/Analyst	1948

6 FIGURE PROFESSIONALI

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

- Project Manager: definisce e gestisce i progetti, adottando e promuovendo metodologie agili; è responsabile del raggiungimento dei risultati, conformi agli standard di qualità, sicurezza e sostenibilità, in coerenza con gli obiettivi, le performance, i costi ed i tempi definiti.
- Enterprise Architect: ha elevate conoscenze su differenti aree tecnologiche che gli permettono di progettare architetture enterprise, sviluppando modelli basati su Enterprise Framework; è responsabile di definire la strategia abilitante per l'evoluzione dell'architettura, mettendo in relazione la missione di business, i processi e l'infrastruttura necessaria.
- Cloud Application Architect: ha conoscenze approfondite ed esperienze progettuali nella definizione di architetture complesse e di Ingegneria del Software dei sistemi Cloud ed agisce come team leader degli sviluppatori ed esperti tecnici; è responsabile della progettazione dell'architettura di soluzione applicative di cloud computing, assicurando che le procedure e i modelli di sviluppo siano aggiornati e conformi agli standard e alle linee guida applicabili
- Cloud Application Specialist: ha consolidate conoscenze tecnologiche delle soluzioni cloud e dell'integrazione di soluzioni applicative basate su un approccio cloud computing based; è responsabile della delivery di progetti basate su soluzioni Cloud.
- Database Specialist and Administrator: È responsabile dell'installazione, dell'aggiornamento, della migrazione e della manutenzione del DBMS; si occupa di strutturare e regolamentare l'accesso ai DB, monitorarne l'utilizzo, ottimizzarne le prestazioni e progettare strategie di backup
- System and Network Administrator: ha competenze sui sistemi operativi, framework di containerizzazione, tecnologie di virtualizzazione, orchestratori e sistemi di configuration e versioning; è responsabile della implementazione di sistemi di virtualizzazione, di container utilizzando anche sistemi di orchestrazione e della manutenzione, della configurazione e del funzionamento dei sistemi informatici di base.
- Developer (Cloud/Mobile/Front-End Developer): Ha competenze di linguaggi di programmazione e di piattaforme di sviluppo, utilizzando le conoscenze di metodologie di analisi e disegno OOA, SOA e REST con UML; assicura la realizzazione e l'implementazione di applicazioni con architetture web-based e cloud-based.
- 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

- Data Protection Specialist: Figura professionale dedicata ad affiancare il titolare, gli addetti ed i responsabili del trattamento dei dati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo.
- System Integration & Test Specialist: Contribuisce in differenti aree dello sviluppo del sistema, effettuando il testing delle funzionalità del sistema, identificando le anomalie e diagnosticandone le possibili cause. Utilizza e promuove strumenti automatici.

7 SICUREZZA

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

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

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.

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.

Polo Strategico Nazionale

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	1684950593
Ragione Sociale	ASL di Latina
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	
Versione	1

VERSIONE CONFIGURATORE	4.1

RIEPILOGO PREZZI				
SERVIZIO		Totale UT		Totale Canone Annuale
Industry Standard			€	238.750,11
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	-
Public Cloud PSN Managed			€	48.776,57
Servizi di Migrazione	€	1.156.469,95		
Servizi Professionali	€	3.460.857,49		
TOTALE	€	4.617.327,44	€	287.526,68

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
VDC_a	IAAS02	IndustryStandard	IaaSPrivateHA	Blade Large	6			€ 48.242,1600
VDC_a	IAAS03	IndustryStandard	IaaSStorageHA	Storage High Performance	100			€ 36.405,0000
VDC_b	DP02	IndustryStandard	DataProtection	Backup	105			€ 34.036,8000
VDC_a	HOUSING05	IndustryStandard	Housing	IP Pubblici /29 (8 indirizzi)	4			€ 261,8000
VDC_c	MGD-OCP-118	PublicCloudPSNManaged	LicensedSQLeOracleHyperscalerTechnology	SQL instances - Gen 2 Exadata Cloud at Customer - Database OCPU - BYOL	20			€ 48.776,5740
VDC_c	IAAS07	IndustryStandard	IaaSStorageHA	Storage HP Encrypted	40			€ 19.948,0000
	CONN01	IndustryStandard	Connettività	Connessione dedicata 1 Gbps	2			€ 17.388,4800
VDC_e	CAAS03	IndustryStandard	CaaS	Open Source (vCPU/anno)	72			€ 32.315,7600
VDC_b	DP03	IndustryStandard	DataProtection	Golden copy	105			€ 40.843,9500
	SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	299		€ 115.817,6500	
	SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	186		€ 46.371,6600	
	SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	130		€ 27.305,2000	
	SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	283		€ 89.244,0500	
	SP-05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	332		€ 82.770,9200	
	SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	279		€ 115.871,4900	
	SP-07	ServiziMigrazione	FiguraMigrazione	Project Manager	739		€ 274.760,2000	
	SP-09	ServiziMigrazione	FiguraMigrazione	Business Analyst	200		€ 59.488,0000	
	SP-10	ServiziMigrazione	FiguraMigrazione	DevOps Expert	120		€ 37.515,6000	
	SP-12	ServiziMigrazione	FiguraMigrazione	System and Network Administrator	155		€ 46.103,2000	
	SP-13	ServiziMigrazione	FiguraMigrazione	Security Principal	150		€ 78.078,0000	
	SP-23	ServiziMigrazione	FiguraMigrazione	Systems Architect	211		€ 102.069,1400	
	SP-24	ServiziMigrazione	FiguraMigrazione	Product/Network/Technical Specialist	242		€ 81.074,8400	
	SP-07	ServiziProfessionali	Rearchitect	Project Manager	13		€ 4.833,4000	
	SP-24	ServiziProfessionali	Rearchitect	Product/Network/Technical Specialist	263		€ 88.110,2600	
	SP-04	ServiziProfessionali	Rearchitect	Cloud Application Specialist	27		€ 8.514,4500	
	SP-23	ServiziProfessionali	Rearchitect	Systems Architect	25		€ 12.093,5000	
VDC_e	IAAS18	IndustryStandard	IaaSSharedHA	Pool 1GB ram aggiuntivo	288			€ 9.308,1600
	SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	443		€ 171.596,0500	
	SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	708		€ 223.267,8000	
	SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	620		€ 230.516,0000	
	SP-21	ServiziProfessionali	SecurityProfessionalServices	Forensic Expert	354		€ 131.617,2000	
	SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	708		€ 210.587,5200	
	SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	531		€ 138.410,4600	
	SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	885		€ 249.791,2500	
	SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	531		€ 197.425,8000	
	SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	443		€ 230.590,3600	
	SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	885		€ 375.036,4500	
	SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	443		€ 187.730,1100	
	SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	354		€ 131.617,2000	
	SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	1948		€ 869.119,6800	

9 Rendicontazione

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

9.1 Servizi di Migrazione

Le attività saranno realizzate secondo quanto esplicitato al paragrafo 5.5. La fatturazione dei servizi avverrà con SAL bimestrali in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali ed in base al Gantt proposto

Codice	Servizio	Tipologia	Elemento	Costo unitario	Q.tà	Costo totale
SP-01	Servizi Professionali	Figura Migrazione	Cloud Application Architect	387,35 €	299	115.817,65 €
SP-02	Servizi Professionali	Figura Migrazione	Database Specialist and Administrator	249,31 €	186	46.371,66 €
SP-03	Servizi Professionali	Figura Migrazione	System Integrator & Testing Specialist	210,04 €	130	27.305,20 €
SP-04	Servizi Professionali	Figura Migrazione	Cloud Application Specialist	315,35 €	283	89.244,05 €
SP-05	Servizi Professionali	Figura Migrazione	Cloud Security Specialist	249,31 €	332	82.770,92 €
SP-06	Servizi Professionali	Figura Migrazione	Enterprise Architect	415,31 €	279	115.871,49 €
SP-07	Servizi Professionali	Figura Migrazione	Project Manager	371,80 €	739	274.760,20 €
SP-10	Servizi Professionali	Figura Migrazione	Business Analyst	297,44 €	200	59.488,00 €
SP-09	Servizi Professionali	Figura Migrazione	DevOps Expert	312,63 €	120	37.515,60 €
SP-12	Servizi Professionali	Figura Migrazione	System and Network Administrator	297,44 €	155	46.103,20 €
SP-13	Servizi Professionali	Figura Migrazione	Security Principal	520,52 €	150	78.078,00 €
SP-23	Servizi Professionali	Figura Migrazione	Systems Architect	483,74 €	211	102.069,14 €
SP-24	Servizi Professionali	Figura Migrazione	Product/Network/Technical Specialist	335,02 €	242	81.074,84 €
					Totali	1.156.469,95 €

Tabella 17: Dimensionamento Sevizi di Migrazione

9.2 Servizi di Rearchitect

Codice	Servizio	Tipologia	Elemento	Costo unitario	Q.tà	Costo totale
SP-07	Servizi Professionali	Rearchitect	Project Manager	371,80 €	13	4.833,40 €
SP-24	Servizi Professionali	Rearchitect	Product/Network/Technical Specialist	335,02 €	263	88.110,26 €
SP-04	Servizi Professionali	Rearchitect	Cloud Application Specialist	315,35 €	27	8.514,45 €
SP-23	Servizi Professionali	Rearchitect	Systems Architect	483,74 €	25	12.093,50 €
					Totali	113.551,61 €

Tabella 18: Dimensionamento Sevizi di Rearchitect

9.3 Servizi di Sicurezza

Codice	Servizio	Tipologia	Elemento	Costo unitario	Q.tà	Costo totale
SP-01	Servizi Professionali	Security Professional Services	Cloud Application Architect	387,35 €	443	171.596,05 €
SP-04	Servizi Professionali	Security Professional Services	Cloud Application Specialist	315,35 €	708	223.267,80 €
SP-22	Servizi Professionali	Security Professional Services	Data Protection Specialist	371,80 €	620	230.516,00 €
SP-21	Servizi Professionali	Security Professional Services	Forensic Expert	371,80 €	354	131.617,20 €
SP-15	Servizi Professionali	Security Professional Services	Junior Information Security Consultant	297,44 €	708	210.587,52 €
SP-20	Servizi Professionali	Security Professional Services	Junior Penetration Tester	260,66 €	531	138.410,46 €
SP-18	Servizi Professionali	Security Professional Services	Junior Security Analyst	282,25 €	885	249.791,25 €
SP-07	Servizi Professionali	Security Professional Services	Project Manager	371,80 €	531	197.425,80 €
SP-13	Servizi Professionali	Security Professional Services	Security Principal	520,52 €	443	230.590,36 €
SP-16	Servizi Professionali	Security Professional Services	Security Solution Architect	423,77 €	885	375.036,45 €
SP-14	Servizi Professionali	Security Professional Services	Senior Information Security Consultant	423,77 €	443	187.730,11 €
SP-19	Servizi Professionali	Security Professional Services	Senior Penetration Tester	371,80 €	354	131.617,20 €
SP-17	Servizi Professionali	Security Professional Services	Senior Security Auditor/Analyst	446,16 €	1948	869.119,68 €
					Totali	3.347.305,88 €

Tabella 19: Dimensionamento Sevizi di Sicurezza

9.3.1 Riepilogo

A titolo esemplificativo si riporta la seguente tabella che rappresenta la stima per l'Amministrazione degli importi economici suddivisi per anno solare, secondo le tempistiche previste nei GANTT ed ipotizzando l'inizio del contratto a Gennaio 2024.

	Anno 2024	Anno 2025	Anno….	Anno 2033
Infrastruttura	143.763,34 €	287.526,68 €	287.526,68 €	287.526,68 €
Servizi di migrazione	1.156.469,95 €			
Servizi di rearchitect	113.551,61 €			
Servizi di sicurezza	223.153,73 €	334.730,59 €	334.730,59 €	334.730,59 €
	1.636.938,63 €	622.257,27 €	622.257,27 €	622.257,27 €

Tabella 20: Riepilogo costi per durata contratto

Servizi di Migrazione (Milestone Based)	Peso	Importo € TOT	Month 2	Month 4	Month 6	Month 8	Month 10
- Analisi & Discovery	35%	404.764,48 €	242.858,69 €		161.905,79 €		
- Setup	30%	346.940,99 €	208.164,59 €		138.776,39 €		
- Migrazione	25%	289.117,49 €		173.470,49 €		115.647,00 €	
- Collaudo	10%	115.647,00 €		69.388,20 €		34.694,10 €	11.564,70 €
Servizi di Rearchitect (Milestone Based)		€ TOT					
- Analisi & Discovery	35%	39.743,06 €	39.743,06 €				
- Setup	30%	34.065,48 €	34.065,48 €				
- Migrazione	25%	28.387,90 €	9.462,63 €	18.925,27 €			
- Collaudo	10%	11.355,16 €		11.355,16 €			
Servizi professionali (avanzamento/task)		€ TOT					
- Security Professional Services	100%	334.730,59 €		55.788,43 €	55.788,43 €	55.788,43 €	55.788,43 €
Totale		€ TOT	534.294,46 €	328.927,55 €	356.470,62 €	206.129,52 €	67.353,13 €

Tabella 21: Consuntivazione costi migrazione