-

Proposta per la realizzazione secondo il modello del Partenariato Pubblico Privato del Polo Strategico Nazionale

Progetto di fattibilità

Signed by Pierpaolo Di Stefano
on 16/12/2021 21:06:58 CET

Firmato digitalmente da:
PIETRO LABRIOLA
Direttore Generale
TIM S.p.A.
Firmato il 16/12/2021 16:17
Seriale Certificato: 446925
Valido dal 01/12/2021 al 30/11/2024
TI Trust Technologies CA

ANDREA QUACIVI
SOGEI S.P.A.
AMMINISTRATORE DELEGATO
16.12.2021
16:39:26 UTC

Firmato digitalmente da

Alessandro Profumo

10 dicembre 2021

Rev. 2.0

Sommario

Indice delle Figure

Lista delle revisioni

Rev.	Data	Descrizione
1.0	27/09/2021	Prima versione del documento
2.0	10/12/2021	Seconda versione del documento. Correzioni refusi e controllo ortografico. Inseriti paragrafi: 1.4 Presentazione del Progetto 1.6 Servizi erogati dai Soci 1.7 Le Partnership della Compagine 1.8 Certificazioni del Personale 2.8 Refresh Tecnologico 2.11.6 Servizio opzionale di moving fisico 4.2.2.6 Connettività dedicata per la migrazione dati 4.2.2.7 Hosting del router di terminazione 5.2.3.1 Sostenibilità energetica e certificazioni

1 PREMESSA

L'Agenzia per l'Italia Digitale è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato. In particolare, promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della Pubblica Amministrazione e nel rapporto tra questa, i cittadini e le imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

Per promuovere l'innovazione digitale nella Pubblica Amministrazione, l'Agenzia per l'Italia Digitale ha attivato un piano complessivo di trasformazione e digitalizzazione delle stesse, ponendo al centro del **modello** strategico la **componente infrastrutturale** (come descritto nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022) con l'obiettivo di **governare** la **trasformazione digitale**.

Le **direttrici evolutive** della componente infrastrutturale sono rappresentata da:

- La **realizzazione** del "**modello Cloud della Pubblica Amministrazione**" e l'applicazione del **principio Cloud First** con cui si intende **facilitare la migrazione dei Servizi delle Pubbliche Amministrazioni verso tale modello**
- La **razionalizzazione ed il consolidamento dei Data Center della Pubblica Amministrazione**, attraverso la progressiva **dismissione dei Data Center obsoleti e inefficienti**, con l'obiettivo di ridurre i costi di gestione delle infrastrutture IT in favore di maggiori investimenti in nuovi servizi digitali
- **L'adeguamento del modello di connettività al paradigma Cloud**, favorendo la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni e la diffusione della connettività nei luoghi pubblici a beneficio delle Pubbliche Amministrazioni, dei cittadini e delle imprese.

In questo contesto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce l'identificazione e la creazione di un nuovo **Soggetto** titolare di un insieme di infrastrutture IT con opportune caratteristiche, **qualificato** (con riferimento alla circolare dell'Agenzia per l'Italia Digitale n. 01 del 14 giugno 2019) **ad erogare alle Amministrazioni, in maniera continuativa e sistematica**:

- Servizi **Infrastrutturali (IaaS, PaaS, BaaS, CaaS)**
- Servizi di **Gestione della Sicurezza IT**
- Servizi di **Disaster recovery** e **Business Continuity**
- **Servizi Professionali** a supporto delle amministrazioni
- Servizi di **Assistenza** ai fruitori dei servizi erogati.

Il progetto che il costituendo ATI realizzerà andrà a gestire l'infrastruttura IT (Data Center e Cloud) con specifiche caratteristiche di affidabilità e sicurezza definite dall'Agenzia per l'Italia

Digitale, ospitando **le applicazioni che supportano l'erogazione di servizi alle Pubbliche Amministrazioni**. Il **Progetto** è destinato a tutti quei **servizi di rilevanza strategica e di interesse nazionale** per i quali non è consigliabile che la gestione dell'infrastruttura e dei dati venga delegata a terze parti.
Nel contesto sopra descritto, Il presente **Progetto di fattibilità** ha lo scopo di proporre i requisiti relativi alla fornitura di un Catalogo di Servizi in oggetto, in quantità, qualità e livelli di servizio adeguati che offra i **servizi** precedentemente **indicati** tramite Data Center **ad alta efficienza e sicurezza** alle **Pubbliche Amministrazioni, principalmente PAC di categoria B**.

La definizione di Pubbliche Amministrazioni Centrali e la classificazione di tale categoria B fa riferimento all'elenco delle Amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm (Legge di contabilità e di finanza pubblica) pubblicato da ISTAT all'interno della Gazzetta Ufficiale (fonte: ISTAT, elenco aggiornato al 30 settembre 2019). I Servizi essenziali sono quelli necessari al mantenimento delle attività economiche e sociali critiche.

Le **Pubbliche Amministrazioni di categoria** B (di seguito indicate come ***PAC*** di tipo B) sono quelle in possesso di Data Center con carenze strutturali e/o organizzative che impedisce loro di garantire la continuità dei Servizi.

Nel presente Capitolo è descritto il contesto in termini di caratteristiche applicative e di ambienti tecnologici e l'oggetto della fornitura, con lo scopo di definire i servizi richiesti; mentre nel **Capitolo 2** sono descritti i Servizi proposti.

Sono altresì indicati nel **Capitolo 3** le caratteristiche di Sicurezza e nel **Capitolo 4** i requisiti della Fornitura, ovvero i requisiti minimi del Servizio, se non diversamente specificato. Le modalità di esecuzione della Fornitura sono descritte nel documento di "*Specificazione delle caratteristiche del Servizio e della Gestione*".

Tutti i termini temporali (giorni, mesi, anni) indicati nel Progetto di fattibilità devono intendersi come "solari", ove non diversamente previsto; la fornitura è articolata in un unico lotto.

Il presente progetto ha l'obiettivo di fornire alla PA una serie di strumenti innovativi a servizio della transizione digitale. Il disegno complessivo si basa sui principi di **sicurezza**, **interoperabilità**, **trasparenza** e **portabilità** delle applicazioni e dei dati.
I pilastri su cui si basa il progetto sono quattro:

- la progettazione e gestione delle infrastrutture, a garanzia della sicurezza, dell'affidabilità, della disponibilità e della scalabilità dei servizi e delle applicazioni gestiti; il progetto prevede l'utilizzo di infrastrutture di Rete, Data Center e interconnessione focalizzate a garantire (by design) le funzionalità sopra riportate. La scalabilità, la disponibilità e la resilienza sono i principi di base delle infrastrutture proposte.
- Il sistema di governance amministrativo e tecnologico che assicura il controllo dei processi, dell'accesso ai dati e della protezione stessa rispetto ai principi di sovranità e di trasparenza. Saranno gestiti i modelli di rilascio di nuovi servizi e nuove tecnologie

seguendo una logica di controllo (sia in termini di sicurezza che di compliance) garantendo i principi di sovranità e di interoperabilità. Il progetto prevede la realizzazione di sistemi di gestione dei rilasci, di controllo degli accessi e di monitoraggio dei funzionamenti a supporto dei principi fondativi.

- Le tecnologie e le scelte architetturali improntate ai principi del multicloud, che permettano di interoperare e utilizzare le varie opzioni in modo agile e flessibile.
- L'inclusione della innovazione proveniente anche da soluzioni di Cloud Provider Internazionali (*Hyperscaler* o CSP), tutelando la titolarità, la sicurezza e la sovranità dei dati.

L'insieme di queste soluzioni ha lo scopo di:

- Offrire per tutta la durata del progetto soluzioni aggiornate in linea con le evoluzioni del mercato.
- La sicurezza del controllo dei dati, dell'accesso e della gestione in territorio italiano di tutta l'infrastruttura. I principi fondatori della proposta rimarranno costanti durante tutta la durata del progetto mentre le tecnologie via via adottate dovranno naturalmente seguire l'evoluzione ed il progresso tecnologico per rimanere sempre all'avanguardia in termini di efficacia e efficienza.
- La scalabilità e la varietà offerta da fornitori come gli *Hyperscaler.*
- L'accesso, reso sicuro e controllato, alle soluzioni *Hyperscaler* da parte del personale del PSN con impatto importante sulla formazione e la crescita delle competenze.
- Una apertura all'ecosistema del territorio con approccio API based per tutti i servizi previsti che permetterà la costruzione di nuovi scenari applicativi *cloud native*.

L'integrazione tra gli *Hyperscaler* e le soluzioni sovrane sarà guidata dai criteri di classificazione del dato. Ogni livello di classificazione che verrà definito dalle strutture competenti, per esempio dall'Agenzia per la Cybersicurezza Nazionale (ACN) potrà esser soddisfatto da una delle diverse soluzioni cloud rese disponibili:

- Soluzioni industry standard, per Hosting, Housing e Private cloud (IaaS, PaaS, CaaS, BaaS);
- Public Cloud PSN Managed, con controllo del software e della gestione;
- Hybrid Cloud on PSN Site;
- Secure Public Cloud - Criptazione dei dati con chiavi nell'esclusiva disponibilità del PSN, sistemi di backup dati e policy di sicurezza;

1.1 Presentazione del costituendo ATI

1.1.1 TIM SpA

TIM è una delle principali realtà ICT in Italia. Lavora per un'Italia sempre più digitale, per rispondere alle esigenze dei cittadini, delle imprese e delle istituzioni, anche nei momenti più difficili. Grazie a interventi realizzati su tutto il territorio, intensificati durante l'emergenza sanitaria per permettere al Paese di non fermarsi durante il lockdown, la fibra ottica di TIM ha connesso già a dicembre 2020 il 90% delle famiglie con linea fissa, con l'obiettivo di chiudere il digital divide in Italia entro il 2021, estendendo a tutti la possibilità di lavorare e studiare a distanza, navigare ad alta velocità e usufruire dei servizi TV e d'intrattenimento. Con l'ultrabroadband mobile LTE TIM viene raggiunto oltre il 99% della popolazione, mentre il 5G TIM raggiungerà la copertura nazionale entro il 2025/2026.

Al centro della strategia del Gruppo i clienti, quasi 100 milioni fra Italia e Brasile, a cui viene offerta una connettività convergente e sempre più ricca: insieme alle telecomunicazioni fisse e mobili anche TV, contenuti digitali per l'entertainment - video, musica, gaming - e soluzioni per la casa intelligente.

Numerosi gli investimenti nell'innovazione e nelle nuove frontiere del cloud ed edge computing, per offrire piattaforme e soluzioni innovative per la digitalizzazione delle imprese, dalle PMI alla grande industria, fino al mondo della pubblica amministrazione e della sanità. Diventano così sempre più smart realtà produttive e territori.

Da 18 anni TIM è presente nei principali indici di Sostenibilità, segno dell'impegno e dell'attenzione agli effetti delle proprie attività sulla comunità e sull'ambiente per una crescita sostenibile. Con il progetto Operazione Risorgimento Digitale - la prima grande scuola di Internet gratuita che opera grazie al contributo di 30 partner e con il sostegno di associazioni di categoria, terzo settore e importanti attori nel campo della innovazione sociale – vengono diffuse competenze digitali nel Paese. Un'iniziativa di cui hanno già fruito oltre 700.000 cittadini. E per quanto riguarda il footprint ambientale, l'azienda ha fissato l'obiettivo di diventare carbon neutral entro il 2030.
Il gruppo si avvale di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e pubbliche amministrazioni, anche in partnership con gruppi di primaria importanza: Noovle è la cloud company di TIM, leading cloud enabler e Centro di Eccellenza a supporto della trasformazione digitale delle aziende pubbliche e private italiane; Sparkle, primo fornitore di servizi wholesale internazionali in Italia e fra i primi 10 a livello globale, con una delle più grandi e avanzate reti al mondo; Olivetti è il polo digitale con focus sullo sviluppo di soluzioni Internet of things, Telsy opera nel settore della cybersecurity.

I numeri di TIM al 30 settembre 2020:

- 30,2 milioni le linee mobili in Italia
- 17 milioni gli accessi totali alla rete fissa
- 51,2 milioni le linee di TIM Brasil
- 52.480 il personale, di cui 42.827 in Italia

1.1.2 CDP Equity S.p.A.

CDP Equity S.p.A. (di seguito anche "CDP Equity" o la "Società"), costituita nel 2011 con il nome Fondo Strategico Italiano S.p.A. e rinominata in CDP Equity nel 2016, è un investitore paziente di lungo periodo e agisce secondo logiche di mercato. Gli interventi in settori strategici, con ritorni adeguati, sono connaturati alla sua missione di sostenere lo sviluppo del Paese. CDP Equity, che è una realtà controllata al 100% dal Gruppo CDP, opera acquisendo prevalentemente quote di minoranza in imprese di rilevante interesse nazionale, che siano in equilibrio economico-finanziario e presentino adeguate prospettive di redditività e sviluppo

CDP Equity investe in aziende di rilevante interesse nazionale, attraverso partecipazioni dirette e indirette. Mette a disposizione capitali per lo sviluppo a lungo termine di organizzazioni in settori chiave per favorire l'innovazione in tecnologie e infrastrutture indispensabili alla crescita del sistema Paese. Attraverso partecipazioni in fondi, e in fondi di fondi, supporta l'ecosistema imprenditoriale italiano. È inoltre un investitore di riferimento negli asset alternativi. In particolare, CDP Equity, che ad oggi ha investito complessivi 4,9 miliardi di euro, effettua:

- ***Investimenti Diretti*** intervenendo, in base al proprio statuto, in aziende che operano in settori strategici per lo sviluppo del Paese e in grado di generare impatto rilevante sull'economia italiana. Per favorire percorsi di consolidamento, espansione e internazionalizzazione, gli interventi di CDP Equity mirano ad intercettare i più rilevanti *mega-trend*: dalla transizione energetica alla *digital transformation*, dall'industria 4.0 al commercio internazionale. Restano al di fuori del perimetro gli investimenti in *holding* finanziarie di partecipazioni diversificate. Attualmente CDP Equity detiene partecipazioni dirette in 14 società di cui 4 sono società quotate.
- ***Investimenti Indiretti*** agendo come investitore *cornerstone* in fondi diretti e fondi di fondi gestiti dalle società di *asset management* di cui è azionista, garantendone la piena autonomia operativa e gestionale. CDP Equity agisce seguendo una rigorosa disciplina di investimento con un processo che prevede un'attenta attività di negoziazione e *due diligence* (con particolare attenzione agli aspetti ESG) e gestione dei fondi partecipati. Attualmente CDP Equity detiene partecipazioni in 5 SGR e ha investito in 7 fondi gestiti dalle medesime SGR

1.1.3 Leonardo S.p.A.

Con oltre 49.000 dipendenti, Leonardo S.p.A. (nel seguito anche LND) è una delle maggiori realtà industriali internazionali operanti nei settori Aerospazio, Difesa e Sicurezza. Un approccio sostenibile di business e una strategia finanziaria disciplinata sono i pilastri principali sui quali si basa la creazione di valore per tutti gli stakeholder. Nel settore Sicurezza e Digital Transformation opera la Divisione Cyber Security che, sfruttando le sinergie tra information technology, comunicazioni, automazione, sicurezza fisica e digitale, mette a disposizione dei propri clienti know how, processi e tecnologie avanzate. Tale Divisione realizza piattaforme applicative per l'erogazione di servizi digitali, supportando l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle Agende Digitali nazionali ed europee.

Si presenta sul mercato come un provider globale di sistemi, prodotti e soluzioni all'avanguardia in grado di rispondere alla crescente domanda di tecnologie avanzate nei settori della sicurezza, dell'informatica, della protezione di informazioni, infrastrutture e territorio, nonché nella gestione di infrastrutture strategiche. Con circa il 12% dei ricavi del 2020, Leonardo è terza in Europa e quarta nel mondo tra le maggiori aziende che investono in Ricerca e Sviluppo nel settore dell'Aerospazio, Difesa e Sicurezza. Il contributo di Leonardo alla spesa in Ricerca e Sviluppo totale del Paese è molto rilevante: considerando solo la parte di spesa allocata in Italia, Leonardo rappresenta il 16,8% della spesa in Ricerca e Sviluppo dei settori a tecnologia alta e medio-alta del Paese e il 10,9% del totale degli investimenti diretti in Ricerca e Sviluppo delle imprese manifatturiere italiane. I processi di innovazione sono supportati da 10 LABS a livello internazionale, di cui 6 in Italia. Vanta pluriennali esperienze maturate presso le principali Amministrazioni Pubbliche Centrali e Locali, risultando negli anni spesso aggiudicataria dei principali Contratti Quadro Consip nell'ambito Applicativo, Infrastrutture e Sicurezza finalizzati a indirizzare il processo di Digital Transformation, tra cui il Contratto per l'affidamento di servizi in ambito Sistemi Gestionali Integrati per le Pubbliche Amministrazioni – Lotto 1 (2017-2022). Nel settore Sicurezza opera la **Divisione Cyber Security** che, sfruttando le sinergie tra information technology, comunicazioni, automazione, sicurezza fisica e digitale, mette a disposizione dei propri clienti know how, processi e tecnologie avanzate. Tale Divisione realizza piattaforme applicative per l'erogazione di servizi digitali, supportando l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle Agende Digitali nazionali ed europee. In particolare, vengono offerte soluzioni innovative per l'erogazione di servizi digitali nei seguenti ambiti, svolgendo il ruolo di partner d'eccellenza nel processo di Digital Trasformation:

- ***Soluzioni di Cybersecurity:*** Grazie al nostro know-how nella protezione di paesi e di infrastrutture nazionali critiche, forniamo soluzioni e servizi che garantiscono il massimo livello di protezione e resilienza, incrementando la capacità di anticipare le minacce, controllare i rischi e gestire efficacemente gli attacchi cyber.
- ***Comunicazioni professionali***: Le nostre reti integrate e piattaforme di comunicazioni sicure sono in grado di soddisfare i più stringenti requisiti di affidabilità, anche in situazioni di emergenza, richiesti da agenzie di pubblica sicurezza, protezione civile e infrastrutture critiche.
- ***Sistemi di gestione e controllo***: Progettiamo e sviluppiamo piattaforme integrate di comando e controllo per la sicurezza urbana, la protezione delle infrastrutture critiche e dei grandi eventi, la gestione delle emergenze e il controllo del territorio.
- ***Sistemi di automazione***: Forniamo sistemi di automazione per la gestione dei bagagli negli aeroporti, basati su tecnologia all'avanguardia cross-belt, e sistemi di smistamento, movimentazione e tracciatura di lettere e pacchi per operatori postali e corrieri.

- ***Soluzioni per mercati***: Offriamo soluzioni innovative chiavi in mano, ritagliate sulle esigenze di sicurezza specifiche di ogni mercato, volte a migliorare la sicurezza dei cittadini e l'efficienza e la resilienza di organizzazioni pubbliche, private e delle infrastrutture critiche.

1.1.4 Sogei SpA

Sogei - Società Generale d'Informatica S.p.A. – è la società di Information Technology, partner tecnologico del Ministero dell'Economia e delle Finanze e interamente partecipata dallo stesso, che opera sulla base del modello organizzativo dell'in-house providing.

Nata nel 1976 come società a partecipazione pubblica, in esecuzione di una specifica previsione normativa, per la realizzazione dell'Anagrafe tributaria, Sogei è oggi la "piattaforma digitale" dell'Amministrazione Finanziaria, che offre soluzioni, competenze e asset, all'interno di un'infrastruttura strategica altamente affidabile.

Ulteriori previsioni normative hanno negli anni esteso negli anni la lista delle pubbliche amministrazioni e istituzioni Clienti, ampliando know-how e competenze e rendendo l'Azienda una risorsa unica del Paese, per efficienza, solidità, sicurezza e alta affidabilità, capace di tradurre le esigenze di innovazione dei propri Clienti in benefici per cittadini, imprese e istituzioni. "Semplifichiamo la vita di Noi cittadini" è il Purpose di Sogei ed è insito nella storia, nell'identità e nella cultura. È ciò che l'Azienda mette al servizio e che tiene conto delle esigenze e dei bisogni delle persone. Semplificare la fruibilità dei servizi e, quindi, la vita di tutti, supportando la digitalizzazione della PA per un'Italia più moderna e competitiva.
La Società ha 2.210 dipendenti (dati al 31 dicembre 2020) e una partecipazione di minoranza nella società Geoweb, società in controllo pubblico, costituita insieme al Consiglio Nazionale geometri e Geometri Laureati per offrire servizi IT ai professionisti.

1.2 Glossario

Salva diversa esplicita indicazione, ai termini seguenti, riportati in ordine alfabetico, viene attribuito, ai fini del presente documento, il significato di seguito indicato.

TERMINE	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
Applicazione	Una qualsiasi realizzazione software (ad-hoc o prodotto di mercato) tesa a fornire un insieme di funzionalità alla PA. Solitamente una applicazione è composta da uno o più moduli software e da un database a cui l'applicazione fa riferimento
Costituendo ATI	Associazione Temporanea d'Impresa promotrice del progetto di fattibilità
Committente	Ministero per l'Innovazione Tecnologica e la Digitalizzazione
Contratto	L'atto che verrà stipulato tra la PA e la NewCo PSN, nel quale sono enunciate le regole giuridiche alle quali si dovrà conformare il Servizio

TERMINE	DEFINIZIONE
Centro Servizi	Il Centro Servizi della NewCo PSN rappresenta l'insieme di tutte le infrastrutture fisiche (Data Center), delle componenti hardware e software in essi ospitati e delle risorse destinate all'erogazione dei Servizi oggetto del presente Progetto di fattibilità
CSP	Cloud Services Provider, anche detti *Hyperscaler*, fornitori di servizi di cloud pubblico su scala mondiale
Fornitura	l'insieme dei prodotti software, hardware, dei servizi e di tutto ciò che è richiesto nel presente Progetto di Fattibilità
NewCO	Società di scopo
Servizi professionali	Gestione sistemistica, supporto specialistico ed evolutivo, servizi di sicurezza, servizio di assistenza
SLA	Service Level Agreement, ovvero "indicatori di prestazione chiave", e cioè quegli indicatori che permettono di misurare le prestazioni di una determinata attività o di un determinato processo

1.3 Contesto tecnologico

I Sistemi Informatici delle PA sono costituiti da più sistemi di elaborazione dislocati presso Data Center per lo più ospitati all'interno delle strutture stesse delle PA, interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività).

Le PA hanno da tempo investito nelle architetture open coerentemente con le indicazioni tecnologiche del mercato e dell'Agenzia per l'Italia Digitale, ma la situazione attuale registra una presenza, per esempio, di variegati sistemi operativi quali Linux, Unix, Windows Server 2003, 2008, 2012.

Tale situazione inoltre non garantisce attualmente la continuità operativa dei servizi, né tantomeno l'architettura degli attuali Data Center delle PA è pensata per erogare i servizi di Business Continuity, operando quindi in alta affidabilità con modalità di allineamento active–active Geografico. Inoltre, la costituzione di molteplici data center locali ha generato:

- lock in tecnologico da parte dei Vendor;
- obsolescenza tecnologica per gli elevati investimenti richiesti per mantenere allo stato dell'arte l'infrastruttura;
- difficoltà a gestire la sicurezza delle informazioni non riuscendo a tenere il passo con il rapido evolversi delle minacce informatiche;
- difficoltà ad implementare processi standard di gestione dei servizi ad elevati standard qualitativo dovendo spesso ricorrere a personale esterno, specialmente per servizi critici H24;

- difficoltà a gestire rapidità nella messa in esercizio di nuovi servizi dovendo spesso aspettare l'esito di procedure negoziali per aggiornare o incrementare la capacità del Data Center.

Occorre quindi che le attuali architetture progrediscano dalla situazione attuale per evitare la presenza di alcun "single point of failure", garantendo quindi la ridondanza di tutti i sistemi e le apparecchiature che rivestono carattere di criticità per l'erogazione di un servizio continuo ad alta affidabilità.

Il contesto descritto è quello di riferimento alla data di stesura del presente Progetto di fattibilità. A valle della stipula del contratto, secondo le modalità e le tempistiche indicate al paragrafo 2.11***Servizio di Migrazione, Evoluzione e Professional Services***, ogni PA aderente all'iniziativa fornirà l'elenco aggiornato e dettagliato del perimetro IT e TLC coinvolto nell'affidamento dei servizi oggetto di gara.

1.4 Presentazione di Progetto

Questo paragrafo vuole dare una visione complessiva dell'intero progetto.

I principi che lo costituiscono sono dettagliati nei successivi e puntuali capitoli che ne descrivono servizi e caratteristiche.

La nostra Compagine è stata costituita per garantire l'aderenza nativa ai principi di disegno del PSN e per dare garanzie di solidità tecnica e finanziaria al progetto ed è composta da:

Istituto Nazionale di Promozione, abilitatore della politica industriale del paese attraverso investimenti in settori strategici quali le infrastrutture di rilevanza critica.

Socio a garanzia del controllo dello Stato e del supporto agli investimenti e al dialogo con la PA.

Leader nel settore della sicurezza tecnologica tra i primi 10 gruppi al mondo per expertise sui temi di digital security.

Socio industriale con significativa expertise in termini di security.

Player di riferimento per la fornitura di servizi informatici e di consulenza ICT alla Pubblica Amministrazione.

Socio industriale con expertise nel servire la PA.

Uno dei più importanti gruppi Telco al mondo, market leader in Italia nei servizi Cloud, Data Center e di connettività per la PA (11% quota di mercato).

Partnership industriale con Google in ambito cloud, per garantire trasferimento tecnologico e know how.

I principi che hanno ispirato il disegno del PSN sono:

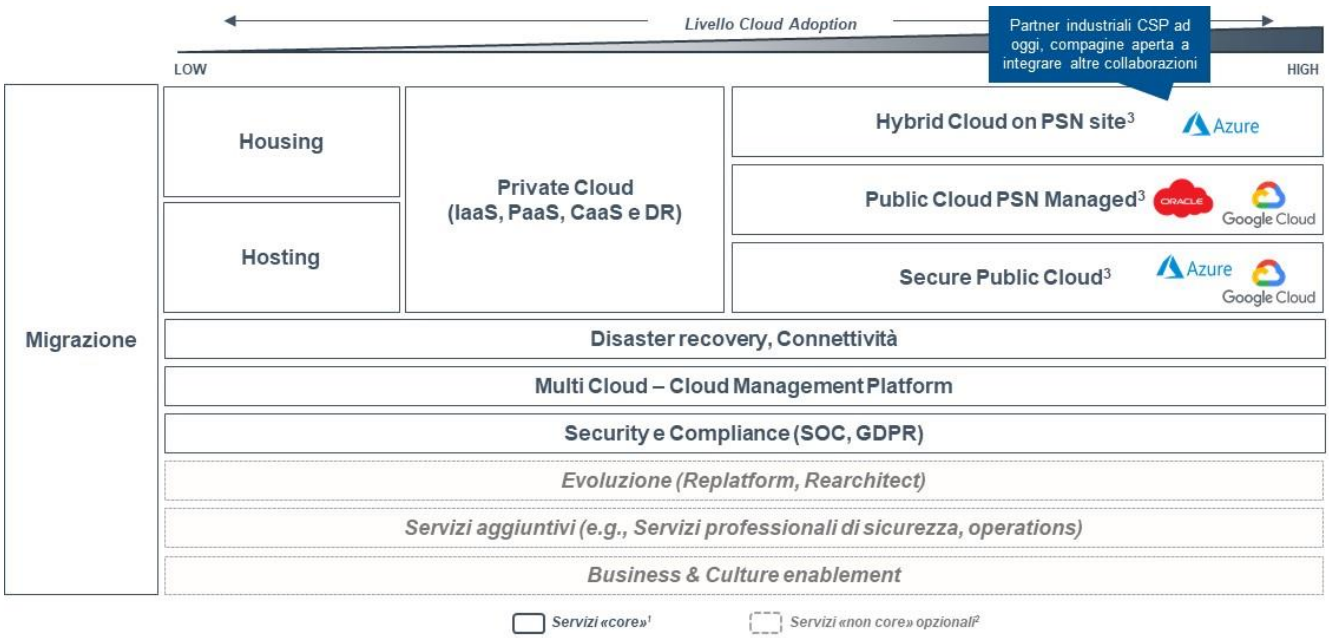
- **Sovranità digitale e controllo statale**: garantire il controllo del PSN in capo allo Stato.
- **Sicurezza**: assicurare un presidio tecnologico e operativo in grado di garantire i più alti standard di sicurezza.
    - **Fisica** (e.g. disaster recovery, business continuity, controllo accessi, etc..);
    - **Informatica** (e.g. prevenzione e risposta attacchi cyber, data protection, identity access management, etc.).

- **Innovazione**: pieno accesso alle migliori soluzioni tecnologiche per le infrastrutture data center, la connettività, le piattaforme e i servizi cloud, garantendo trasferimento tecnologico di esperienze e know how con i leader globali.
- **Conoscenza della PA**: dimestichezza con le dinamiche di fornitura di servizio, velocità nel rispondere alle necessità e referenze pregresse.

La proposta della Compagine è fondata su alcune assunzioni, di seguito elencate:

- **4 Data Center**, a partire da circa 800 mq. disponibili a T0 (comprensivi di connettività) fino a 2900 mq nello scenario di massima adesione.
- **Massima flessibilità** nell'offerta di servizi (housing, hosting, private cloud, hybrid cloud, public cloud).
- **Sovranità del dato**, elevati livelli di sicurezza (sarà allineato alla direttive ACN).
- **Società di scopo (NewCo PSN)**, operativa con circa 100 FTE a regime.
- **Adesioni** delle PA stimate non al 100% del perimetro.
- **Durata** della Convenzione per singola PA aderente di 10 anni.
- **Refresh tecnologico** all'anno 5.
- **Garanzia di evoluzioni tecnologiche** (nuovi servizi) e revisione dei prezzi secondo l'andamento del mercato.

L'offerta del PSN è costruita per essere la più ampia possibile per permettere a tutte le PA di scegliere i servizi più idonei alle loro necessità.

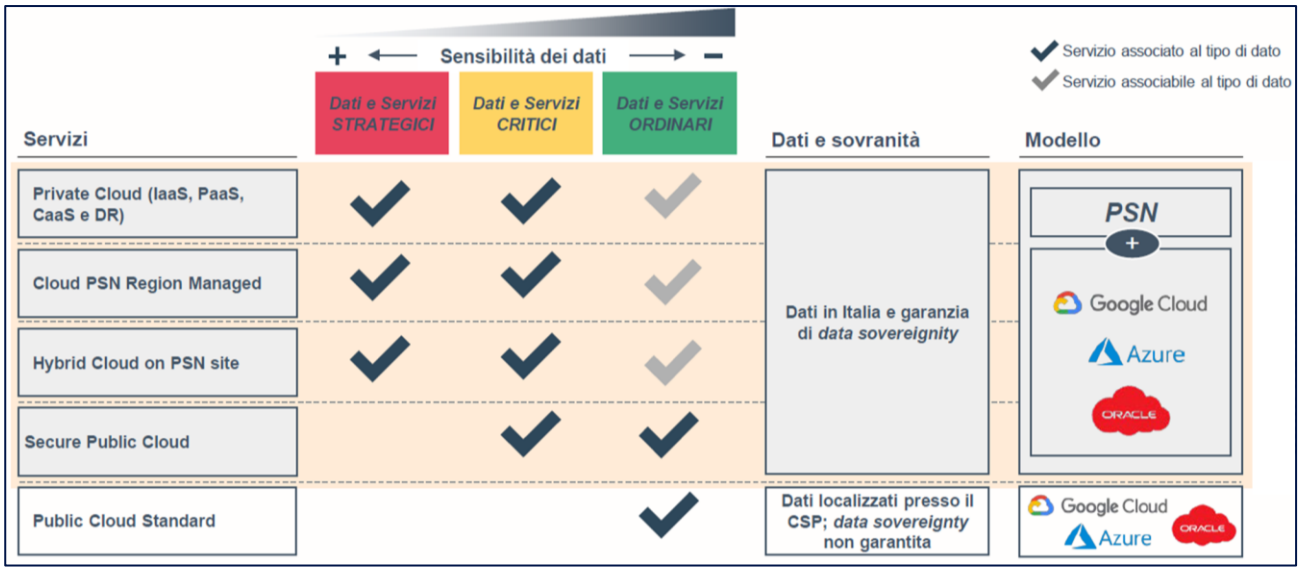


Note: (1) Servizi per razionalizzazione, «messa in sicurezza» e adeguamento tecnologico e innovazione delle infrastrutture IT delle PA; (2) Servizi a disposizione delle PA, funzionali all'ulteriore evoluzione dei servizi (o a bisogni contingenti); (3) In grado di operare in modalità private, hybrid e public.

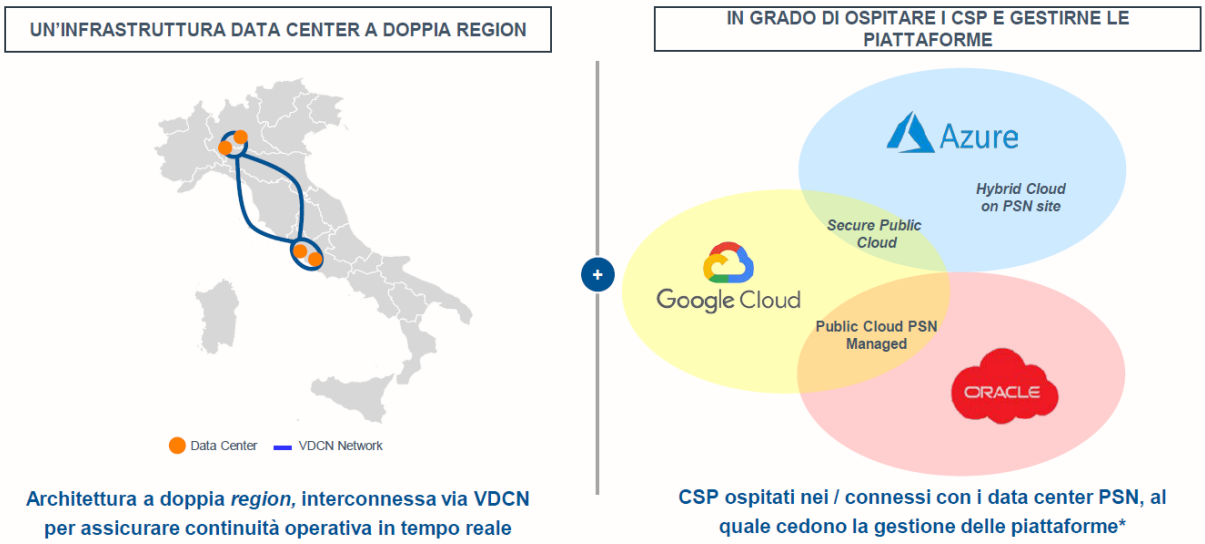
Di seguito sono sintetizzati e schematizzati i servizi "core" e "no core" offerti alle PA.

Servizi		Descrizione (Servizi «core» / Servizi «non core» opzionali)
Migrazione		• Migrazione end-to-end **chiavi in mano** sia **fisica** che **virtuale** (dall'analisi applicativa al test sui nuovi ambienti e messa in produzione)
Housing e Housing		• Servizi di **gestione infrastrutturale** tradizionali. In caso di housing, il cliente utilizza lo spazio attrezzato di proprietà del provider in cui colloca i propri server, a differenza dell'hosting, in cui il cliente ha la possibilità di noleggiare i server di proprietà del provider
Private Cloud	IaaS dedicato	• Offerta di **infrastruttura virtualizzata** (capacità computazionale e storage) in modalità cloud, on demand e *as a service*, con possibilità di noleggiare server virtuali di proprietà del provider
Private Cloud	Iaas Shared	• Servizi **on demand private cloud infrastrutturale** (area Cloud dedicata per il cliente)
Private Cloud	CaaS e DR	• **CaaS (Container as a Service):** servizio cloud con possibilità di sviluppare applicazioni in ambienti «cloud native»; **DR (Disaster Recovery):** servizio back up dei contenuti informativi conservati in Cloud
Private Cloud	PaaS	• Messa a disposizione di **piattaforme** in grado di erogare **elementi applicativi e middleware** come servizio (database, big data, AI)
Soluzioni con CSP	Hybrid Cloud on PSN site	• **Servizi del CSP** (Cloud Service Provider) **hybrid** (combinazione di Cloud pubblico e privato mediante un'infrastruttura integrata) e **installati sull'infrastruttura locale** del PSN
Soluzioni con CSP	Public Cloud PSN Managed	• **Portfolio dei servizi CSP erogato da «Region» dedicata al PSN**, con separazione logico/fisica e operata e controllata da personale PSN
Soluzioni con CSP	Secure Public Cloud	• Servizi di **messa in sicurezza** di un sottoinsieme del **portafoglio di offerta relativo a un CSP**
Servizi aggiuntivi (Security Profess. Services incl. Security Compliance)		• Servizi professionali per il **miglioramento della sicurezza delle infrastrutture** e delle **applicazioni della PA**
Evoluzione (Re-platform, Re-architect)		• Servizi professionali evolutivi volti al **ridisegno delle applicazioni in ottica Cloud**
Servizi aggiuntivi (IT infr. Service Operations)		• Servizi di **Managed Services** per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni
Business & Culture enablement		• Servizi di **formazione / consulenza alle PA** per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità

Attraverso il PSN ogni PA potrà scegliere le soluzioni cloud più adatte a garantire innovazione ma anche privacy, sicurezza, compliance, efficienza e sovranità del dato.



Il rapporto industriale con i Cloud Services Provider (CSP) è profondo: risiederanno nei data center del PSN e sono pronti a cedere al PSN la gestione delle loro piattaforme.



Questo rapporto industriale permetterà al PSN di erogare un set di servizi Cloud in collaborazione con i CSP.
Il PSN **offrirà soluzioni di sicurezza in linea con le normative, le best practice italiane, europee ed internazionali** secondo il modello descritto in figura. Per una descrizione più dettagliata si rimanda al § 3 Sicurezza.

FISICA	Presidio strutture	• **Videosorveglianza** integrata, **vigilanza** armata 24/7, **sensori** perimetrali, **standard ISO 27001**, …
	Controllo accessi Identità e permessi	• Restrizioni al personale autorizzato con **verifica multi-layer credenziali accesso** (one time password, parametri biometrici…)
	Protezione HW	• **Compartimentazione accessi** anche all'interno del DC, verifica movimentazione HW basata su seriali…
LOGICA	Endpoint & Data Protection	• Crittografia dei dischi, Software Antivirus e EDR, gestione dei dispositivi mobili, File Integrity Monitoring
	Identity, Access & Key Management	• Identity&Access Governance, Privileged Access Management, Authentication Management e MultiFactor Authentication. Gestione delle chiavi di cifratura e HSM
	Infrastructure & Network Security	• Segregazione degli ambienti, Accesso controllato, Hardening, Next Generation Firewall, Accesso Zero Trust, e-Mail&Web Security, Network Access Control.
ORGANIZZATIVA	Piano di Sicurezza	• Redazione, implementazione e manutenzione di un **piano di sicurezza**
	Conformità	• Processi di conformità **a normative di sicurezza italiane ed europee**, e a **standard e best practice**
	Organizzazione per la gestione della sicurezza cibernetica	• Definizione della costituency, erogazione di servizi di sicurezza da **SOC** e **CERT** specializzati

Nota: fonte dati sulla situazione attuale della PA da MID, su base censimento.

Verrà predisposta un'unita organizzativa caratterizzata da specifici elementi di autonomia e indipendenza, al fine di garantire e assicurare la tutela delle infrastrutture e dei servizi considerati essenziali agli interessi e alla sicurezza nazionali.
La governance e la gestione sarà affidata a personale altamente competente in materia di Cyber Security. L'unità organizzativa di sicurezza ha l'obiettivo di garantire l'attuazione dei massimi protocolli di sicurezza attraverso:

- lo sviluppo del **Piano di sicurezza**

L'Organizzazione di Sicurezza predisporrà uno specifico e dettagliato Piano di Sicurezza redatto in conformità con i criteri di accreditamento AgID relativi ai PSN, che conterrà:

- una sintesi delle normative di riferimento applicabili;
- una generale ricognizione degli asset informatici;
- le criticità, anche solo potenziali;
- gli obiettivi di sviluppo, manutenzione e gestione, atti a garantire la corretta erogazione dei servizi;
- le risorse strumentali ed economiche necessarie.

- **Attività di controllo**

All'Organizzazione di Sicurezza saranno attribuiti compiti di controllo e supervisione in relazione alla corretta implementazione nei vari ambiti operativi.
Il Responsabile di tale organizzazione potrà essere individuato in accordo con le autorità istituzionali competenti e sarà dotato di specifici requisiti (es. NOS, cittadinanza italiana).

- **Operations**

Sul piano delle Operations, l'Organizzazione di Sicurezza, svilupperà, in particolare, le funzioni di **Security Operation Center (SOC)** e di **Computer Emergency Response Team (CERT)** e garantirà tutti i livelli di sicurezza previsti dalle normative vigenti, la presenza di un ambiente sicuro e protetto e la protezione dei dati personali trattati.

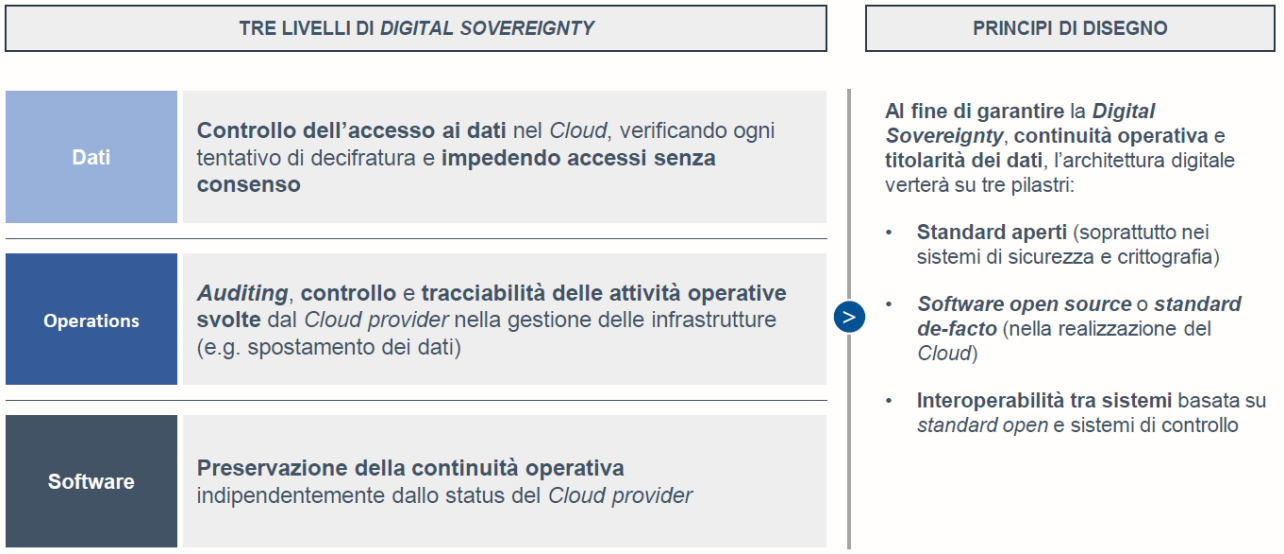
End Point Security	Real Time Security Monitoring
Identity & Access Management	Training & Awareness
Key Management	Incident Response
Security Platform Management	Security Testing & Vulnerability Management
Security Policy management & Enforcement	Threat Intelligence & Infosharing

Attività operative

La proposta di questa compagine rappresenta **un'offerta di servizi gestiti ricca**, in grado di accompagnare la PA lungo tutto il journey del cloud, dalla migrazione all'assistenza.

FASI PROGETTUALI	TRASFERIMENTO KNOW HOW
Disegno e Implementazione	▪ **Assessment** delle infrastrutture IT, **progettazione** dell'infrastruttura, dell'architettura e **servizi di consulenza** per piani di migrazione e supporto alla trasformazione digitale **in collaborazione con la PA** ▪ **Gestione operativa eseguita con la PA e per la PA** garantendo trasferimento di know how verso i **dipendenti pubblici** che utilizzeranno i servizi del PSN
Utilizzo giornaliero dei servizi	▪ Nella fase di execution, **graduale accompagnamento della PA** nel modello di gestione attività (monitoraggio, gestione infrastrutturale, ottimizzazione costi, …) **a regime** ▪ **Il PSN supporterà il personale della PA** nell'apprendimento necessario all'utilizzo di tool che consentano **la gestione dell'infrastruttura Cloud in autonomia** (e.g., piattaforme di self-provisioning)

Al termine della concessione, alla PA sarà garantita la proprietà dei dati e la continuità operativa in base ai principi della Digital Sovereignty.



Si riportano di seguito i **punti di forza della proposta presentata** che sono supportati dalle soluzioni di seguito descritte:

1. **Public Cloud PSN Managed (Managed Region)**: **collocata** negli stessi **Data Center** delle soluzioni **Industry Standard**, controllata e gestita da **personale PSN italiano**, con rilasci degli **aggiornamenti SW controllati e certificati**.

2. **Secure Public Cloud**: le chiavi di **crittografia non risiedono** all'interno del **cloud CSP** ma sono **esterne**, sotto il totale **controllo del PSN**, duplicate per garantire **affidabilità**, **ridondanza** e **ottimizzazione** dei **tempi** di accesso. Nel caso di Secure Public Cloud con CSP Google la gestione è LAN to LAN (stesso Data Center).

3. **Hybrid Cloud on PSN Site**: **Architettura hybrid controllata e certificata**, controlli sulla "frontiers" di interconnessione con la componente Public, collocata negli stessi Data Center delle soluzioni Industry Standard.

4. **Sintesi delle proposte CSP**: **3 diverse possibili soluzioni**, tutte e tre contemporaneamente attive, **3 CSP complessivamente coinvolti con 2 CSP** a presidio di ogni **soluzione** (la soluzione di Oracle per la Region è funzionalmente sovrapponibile alla proposta Hybrid). Massima **indipendenza** dal **singolo CSP**, nessun servizio è erogato in modalità esclusiva.

5. **Caratteristiche societarie**: circa **100 persone assunte direttamente**, **management** scelto per **professionalità** e **garanzia** di **indipendenza** rispetto ai costi. Procedure di Sicurezza e

Compliance dedicate ed esclusive per la gestione del PSN. Disponibilità a **dotare** tutto il **personale** del **NOS** e la società del **NOSI**.

6. **Soci Industriali**: la forza della compagine, **Asset proprietari** (Data Center), **capacità** di fornire **connettività fissa** e **mobile** (5G), **Adozione** di **soluzioni Edge** per la prossimità, **garanzia** di un **player** attivo sulla **Sicurezza Nazionale**, le **migliori esperienze di migrazione** al **Cloud** della **PA**.

7. **Ruolo di CDP** come **investitore istituzionale** di garanzia che "ha **selezionato**" la **miglior formazione** possibile anche in termini di "**sovranità**" della proposta.

1.5 Oggetto della Fornitura

1.5.1 La NewCo

Il costituendo ATI al fine di mettere a disposizione delle Amministrazioni un servizio a loro dedicato, in grado di aiutarle e supportarle in tutte le fasi di vita di un contratto, **intende costituire,** a seguito dell'aggiudicazione della relativa gara, **una società di scopo** ("**NewCo**") opportunamente dimensionata. Tale nuova società sarà organizzata con Strutture Tecniche, Strutture Operative, di Sales & Marketing e figure di Staff.

Nel dettaglio le Strutture Tecniche si occuperanno degli ambiti relativi a:

- Network;
- Security;
- IT Infrastructure e Housing;

le Strutture Operative si occuperanno di:

- Management;
- Governance;
- Logistica;
- Project Management;
- Facilities DC;
- eProcurement.

Le funzioni di Sales & Marketing saranno impiegate nella promozione e nella commercializzazione dei servizi PSN oltre che nel Marketing dei servizi.
Le funzioni di staff ricomprendono ruoli quali:

- CFO;

- Audit;
- BD&S;
- Legal;
- Human Resource;
- Rapporti con Stakeholder;
- IT Staff.

La NewCo avrà ovviamente un proprio Amministratore Delegato ed un Presidente.

La NewCo PSN ha dimensionato la NewCo prevedendo un impiego di **oltre 80** persone per adempiere ai ruoli ed alle attività sopra indicati; ovviamente la NewCo si avvarrà anche di personale esterno in supporto al personale interno.

La NewCo PSN oltre al personale (interno ed esterno) si avvarrà del contributo dei soci industriali Leonardo, Sogei e TIM.

Nel prosieguo del presente Progetto di fattibilità si farà sempre riferimento alla NewCo come soggetto che avrà la responsabilità di erogare i servizi. In attesa di definire la ragione sociale della società di scopo, verrà denominata "**NewCo PSN**".

1.5.2 Tipologia di servizi erogati dalla NewCo PSN

La Fornitura prevede l'erogazione alle PA, secondo lo standard ISO 20001 per la gestione dei servizi IT in maniera continuativa e sistematica, di un Catalogo di Servizi, dedicati e con estremo focus su sicurezza, connettività ed affidabilità. I servizi offerti, oltre a quelli trasversali riportati di seguito, saranno suddivisi in "*Core*" e "*no Core*" (o Opzionali) e vengono individuati i **Service Elements** in relazione alle modalità di erogazione dei Servizi Infrastrutturali.

- Servizi di **Gestione della Sicurezza IT, a standard ISO 27001**
- Servizi di **Disaster recovery** e **Business Continuity, a standard ISO 22301l**
- Servizi di **Assistenza** ai fruitori dei servizi erogati
- **Console Unica** di gestione.

Con ✓ indichiamo i Service Elements **necessari** in relazione alla modalità prevista.
I servizi trasversali sono i seguenti:

Servizi		Industry Standard						Hybrid Cloud on PSN Site	Secure Public Cloud	Public Cloud PSN-Managed
		Housing	Hosting	IaaS	CaaS	PaaS	BaaS			
Facility		✓	✓	✓	✓	✓	✓	✓	✓	✓
Connectivity		✓	✓	✓	✓	✓	✓	✓	✓	✓
Operational Continuity		✓	✓	✓	✓	✓	✓	✓	✓	✓
Maintenance & Helpdesk		✓	✓	✓	✓	✓	✓	✓	✓	✓
IT Infrastructure			✓	✓	✓	✓	✓	✓	✓	✓
Service & SLA Management		✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitoring			✓	✓	✓	✓	✓	✓	✓	✓
Operational & Security Management	**Physical**	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Network	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Hardware		✓	✓	✓	✓	✓	✓	✓	✓
	Hypervisor			✓	✓	✓	✓	✓	✓	✓
	Operating System			On-Demand	✓	✓	✓	Only for PaaS and CaaS Services	Only for PaaS and CaaS Services	Only for PaaS and CaaS Services
	Middleware					✓	✓	Only for PaaS Services	Only for PaaS Services	Only for PaaS Services
	Runtimes					✓	✓	Only for PaaS Services	Only for PaaS Services	Only for PaaS Services
	Application						✓			
	Data						✓			

1.5.3 Servizi Core

Di seguito si riporta l'elenco dei servizi individuati come Core:

- Servizi **Infrastrutturali on-demand:**
  - **Industry Standard (Hosting, Housing, IaaS, PaaS, BaaS, CaaS);**
  - **Public Cloud PSN Managed;**
  - **Secure Public Cloud;**
  - **Hybrid Cloud on PSN Site;**
- Servizi di **Migrazione**

1.5.4 Servizi no Core

Di seguito si riporta l'elenco dei servizi individuati come Opzionali:

- **Servizi di Evoluzione (Re-Platform e Re-Architect)**
- **Professional Services**
- **Business & Culture Enabling**

1.6 Servizi erogati dai Soci

La tabella che segue elenca i servizi/attività erogati dai Soci con relativa descrizione di fornitura.

Servizi/Attività erogati dai Soci al PSN	Descrizione della fornitura
1. Spazi Attrezzati	Canone relativo a: •Affitto di 4 Data Center attrezzati e dedicati al PSN certificati Tier IV di cui 2 con disponibilità di sale Tier III, localizzati in doppia Region per garantire business continuity e soluzioni di Disaster recovery in logica High Availability per permettere un Backup real-time. •Acquisto di cablaggi in componente attiva (e.g. configurazione VLAN, firewall, router) e in componente passiva (e.g. cavi, switch).
2. Connettività	•Connessione ad alta velocità per il collegamento dei Data Center (intra region e infra region). •Servizio di protezione degli IP da cui le Amministrazioni erogheranno i propri servizi attestati sull'infrastruttura Industry Standard. Servizio progettato per «surgical mitigation», agendo sul traffico per singolo IP attaccato.
3.Energia	Fornitura di energia elettrica per l'infrastruttura IT del PSN. Il servizio viene erogato dai soci, i quali possono utilizzare accordi in essere con i propri fornitori a condizioni vantaggiose per il PSN.

Servizi/Attività erogati dai Soci al PSN	Descrizione della fornitura
4.COPS - servizi di gestione cliente (Help Desk di primo livello)	Servizio di Help Desk di primo livello dedicato ai clienti del PSN. Il servizio viene erogato da uno dei soci che, operando servizi di Help Desk di grandi dimensioni, può generare benefici per il PSN in termini di efficienza, qualità e scalabilità.
5. Service Management - servizio di gestione del cliente	Servizio di gestione delle interazioni con le PA composto da referenti dedicati per ogni amministrazione per attività di governance del servizio, reportistica e escalation delle richieste cliente. Il servizio viene gestito da un socio che già possiede una struttura consolidata di Service Management in ambito technology.
6. Security Operations	Servizio di Security Operations (inclusivo di attività di SOC) fornito dal socio con maggiore esperienza ed asset in ambito sicurezza in grado di generare benefici per il PSN in termini di efficienza, qualità e scalabilità.
7. Sicurezza CERT	Gestione di incidenti informatici sia in modalità proattiva (gestione delle vulnerabilità e delle minacce e prevenzione) sia in modalità reattiva (gestione tempestiva degli incidenti). Servizio erogato da un socio con infrastruttura CERT già predisposta e operativa.
8. Servizi Professionali di Sicurezza	Attività di Strategy & Compliance, assessment di sicurezza su infrastruttura e parco applicativo e supporto alle Operations per il mantenimento degli elevati standard di sicurezza.
9. Secure Public Cloud	Servizio di Key management, Template, Backup e di erogazione del servizio di Secure Public Cloud, progettato tramite accordo industriale tra soci e i CSP (Azure e GCP).
10. Hybrid Cloud on PSN Site	Gestione operativa del servizio e delle attività di sicurezza connesse all'Hybrid Cloud, progettato tramite accordo industriale tra soci e il CSP (Azure)
11. Public Cloud a PSN Managed	Gestione dell'infrastruttura dedicata e relativa manutenzione, analisi di sicurezza e attività di SOC, sviluppo degli «Shim layers» per il collegamento a servizi esterni. Servizio progettato con specifico accordo industriale tra soci e CSP (Oracle e GCP).
12. Business & Culture Enablement	Servizi di formazione / consulenza alle PA per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità. Erogato da un socio con elevata conoscenza dell'infrastruttura digitale della PA.
13. Re-Architect	Servizi professionali evolutivi volti alla riprogettazione dell'architettura delle applicazioni in ottica Cloud. Erogato dai soci con profonda conoscenza dell'ambiente cloud.

Servizi/Attività erogati dai Soci al PSN	Descrizione della fornitura
14. Re-Platform	Servizi professionali evolutivi volti alla riprogettazione delle piattaforme che gestiscono le applicazioni della PA in modo da abilitarne la trasformazione verso il Cloud. Erogato dai soci con profonda conoscenza dell'ambiente cloud.
15. Servizio di migrazione	Servizio di migrazione end-to-end chiavi in mano sia fisica (housing) che virtuale (dall'analisi degli applicativi al test sui nuovi ambienti e messa in produzione) dell'infrastruttura IT della PA verso l'infrastruttura PSN.
16. IT Infrastructure - Controllo produzione (gestione sistemistica)	Servizi di Managed Services per garantire il mantenimento di funzionalità e/o ottimizzazione degli ambienti su cui insistono le applicazioni. Erogato dai soci con ampia esperienza nella gestione sistemistica dei Data Center.
17. IT Infrastructure - Service Operations	Servizi specialistici on demand a supporto delle Operations per la gestione dell'infrastruttura e del parco applicativo cliente. Erogato dai soci con ampia esperienza nella gestione operativa dei Data Center.
18. PaaS Industry	Installazione e manutenzione degli HW e SW necessari per erogare il servizio. Erogato da soci con ampia esperienza in soluzioni AI, Big Data e IAM.
19. Servizi di intra-migrazione	Servizio end-to-end di migrazione da servizi industry standard verso servizi Cloud avanzati per abilitare la trasformazione cloud della PA.

1.7 Le Partnership della Compagine

Il RTI ha in essere molteplici accordi di partnership tecnologiche. Relativamente alle partnership strategiche con i Cloud Services Provider (CSP), anche detti *Hyperscaler*, la situazione è riportata nei paragrafi successivi.

1.7.1 Google Cloud

Partnership con Google

A marzo 2020 TIM e Google Cloud hanno sottoscritto un importante accordo di collaborazione della durata di 5 anni, rinnovabile per ulteriori 5 anni.
L'impegno congiunto di Google e TIM ha previsto la realizzazione di due Region in Italia (per complessive sei Availability Zone) con rilascio progressivo ad iniziare dal primo trimestre 2022. TIM può comunque ospitare altri Cloud provider nei propri Data Center.
L'accordo ha riguardato i seguenti ambiti:

- Il Set-up delle Region GCP (Google Cloud Platform) in Italia;
- L'attività di go-to-market congiunto sulla primaria clientela italiana pubblica e privata;
- La definizione di soluzioni di Edge Cloud;
- L'utilizzo delle soluzioni GCP per l'IT interno di TIM;

- Potenziali upside addizionali.

Le condizioni previste dalla partnership per quanto riguarda le attività commerciali possono essere estese ad altre aree geografiche dove è presente il gruppo TIM, previo accordo tra le parti.
TIM e GCP stanno lavorando congiuntamente per la realizzazione della soluzione a supporto della Region Dedicata GCP per il mercato italiano con uno specifico focus per la realizzazione del Polo Strategico Nazionale che costituirà la prima esperienza in assoluto di questo tipo in Italia per l'intero mercato dei CSP.
Le parti stanno definendo il modello di accesso alle infrastrutture GCP secondo un modello isolato e che garantisca la sovranità delle applicazioni e dei dati. A fronte di questo modello, GCP permette al personale TIM di accedere a specifiche aree di lavoro dedicate alla Pubblica Amministrazione. TIM in questo contesto garantisce il personale adeguato alla copertura, a ricevere il software di GCP, gestirne la messa in produzione e a gestire l'hardware e le parti di ricambio in linea con i più elevati livelli di servizio richiesti dai servizi cloud.
L'accordo della Region Dedicata per il PSN segue quello della Region italiana GCP in termini temporali; TIM fornisce il personale e le soluzioni per gestire in autonomia le tecnologie GCP. Il progetto in questione costituirà un'aggiunta, specifica per il Polo Strategico Nazionale, all'accordo industriale descritto sopra.

Google Cloud Platform (GCP) è una piattaforma di servizi Cloud gestita, altamente scalabile, che consente l'esecuzione di carichi di lavoro in ambienti diversi dalle macchine virtuali (Compute Engine) ai container (Google Kubernetes Engine), fino a soluzioni serverless (CloudRun, AppEngine, Cloud Function).

GCP offre servizi IaaS, PaaS e SaaS su vasta scala, che spaziano dall'intelligenza artificiale al machine learning, dal datawarehousing a soluzioni di DevOps, dall'Api Management a soluzioni che facilitano scenari ibridi. La connessione con gli ambienti on-premise, disponibile in diverse modalità (Cloud VPN, Dedicated e Partner Interconnect, Peering) è assicurata da una dorsale di rete proprietaria in fibra ottica, in continua espansione, ad elevate prestazioni, che collega i vari data center distribuiti su scala globale, organizzati in zone di disponibilità e Region. Sono di prossima apertura le due Region italiane a Milano e Torino. Google Cloud Platform può contare su oltre 100 punti di presenza in 15 regioni globali. Con il Virtual Private Cloud (VPC) è possibile connettere le proprie risorse GCP o isolarle l'una dall'altra. Attraverso Cloud Delivery Network (CDN) il contenuto viene distribuito attraverso punti di presenza a livello edge e il servizio di Cloud Load Balancing può bilanciare il traffico HTTP(S), TCP/SSL e UDP. La migrazione in tempo reale di macchine virtuali e una varietà di backup ridondanti assicurano un'archiviazione sempre disponibile. Google Cloud dispone inoltre di un'articolata piattaforma per la gestione dei dati, dalla creazione, alla trasformazione all'analisi.

Google ha da tempo iniziato lo sviluppo di servizi per indirizzare le richieste di sovranità digitale (relative alle tre dimensioni dei dati, delle operazioni e del software). In questo ambito sono quattro le soluzioni offerte in cui il controllo dei dati e delle operazioni viene spostato progressivamente dal Cloud Service Provider ad un partner qualificato o all'amministrazione stessa:

- Public Cloud;
- Secure Public Cloud;

- Partner Managed Cloud;
- GPC.

I servizi di Google Cloud assicurano che il dato sia crittato sia at rest che in transit e, tramite il Confidential Computing, anche in memoria.

L'offerta Public Cloud di Google, già nativamente dotata del servizio di Key Management con gestione delle chiavi da parte di Google stessa o del cliente anche in moduli HSM, è stata arricchita con le funzionalità di External Key Manager (EKM), servizio che consente di conservare le chiavi crittografiche affidandole ad un operatore esterno a Google, realizzando così un Secure Public Cloud. A questo si aggiunge la funzionalità di Key Access Justification che consente l'auditing degli accessi alle chiavi con la possibilità di definire alert in caso di accesso non giustificato.

La soluzione Trusted Partner Cloud prevede la gestione da parte di un partner qualificato di una istanza della Google Cloud Platform, che gira in ambienti sotto il controllo del partner stesso, siano essi una porzione di un data center Google acceduto solo dal partner o in uno spazio dedicato di proprietà del partner. L'accesso a tali ambienti è precluso ai dipendenti Google, se non preventivamente autorizzati dal partner. Il partner è proprietario del Certificate of Authority, dei sistemi di identità, dell'infrastruttura e ha in custodia fisica l'intero hardware. Tutti i dati in transit e at rest sono criptati con chiavi gestite ed in possesso del partner che ha diversi livelli di controllo e della sicurezza: sicurezza applicativa, sicurezza del trasporto, controlli crittografici, sicurezza delle macchine, sicurezza fisica, rete logica e fisica. Google mantiene solamente la gestione dell'hardware e del software, assicurando i necessari aggiornamenti.

Per una gestione completamente disconnessa Google propone la soluzione Google Private Cloud, che consente, in un ambiente multi-tenant di proprietà del cliente o di un partner o in co-location, l'operatività della Google Cloud Platform su hardware certificato. Un cloud privato che offre le funzionalità e le capacità avanzate di Anthos, il servizio per la gestione centralizzata e multi cloud di ambienti containerizzati, combinate con un insieme di servizi della piattaforma e di terze parti forniti in una soluzione chiavi in mano che include l'infrastruttura (l'elaborazione, lo storage e il networking). Questa soluzione, pre-certificata e preconfigurata, offre al contempo livelli di servizio più elevati e garantiti, nonché la flessibilità di un modello autogestito o gestito da partner.

1.7.2 Microsoft Azure

Partnership con Microsoft

A maggio 2021 Leonardo e Microsoft hanno sottoscritto un Memorandum of Understanding volto a dare il via ad una collaborazione industriale che ha come finalità anche la realizzazione di progetti per la trasformazione digitale della Pubblica Amministrazione Italiana e per le infrastrutture critiche nazionali, focalizzandosi sulla protezione dei dati e l'impiego di tecnologie e soluzioni cloud avanzate, come quelle inserite nella proposta per il futuro Polo Strategico Nazionale (PSN).
Nell'accordo, Leonardo si candida al ruolo di System Integrator e responsabile della Cyber Security per la trasformazione digitale e il consolidamento dei data center della Pubblica Amministrazione, mentre Microsoft mette a disposizione tecnologie e servizi avanzati di produttività, sicurezza, cloud e automazione dei processi, per consentire l'accelerazione digitale della pubblica amministrazione e delle aziende Italiane.

In base a questo MoU, il personale di ingegneria di Leonardo e Microsoft ha collaborato in modo esclusivo alla definizione e alla progettazione delle migliori soluzioni per erogare servizi per il cloud cifrato (Secure Public Cloud) e per l'ibrido su licenza (Hybrid Cloud on PSN Site) all'interno del PSN. Questa collaborazione, facendo leva sulla possibilità di conoscere in anteprima le evoluzioni dei prodotti Microsoft, consente di inserire soluzioni più sicure e rende più ampia l'offerta prevista dal PSN.
In particolare, la conoscenza delle evoluzioni future delle soluzioni di confidential computing del cloud Azure ha permesso di inserire nella proposta del 29 settembre u.s. l'applicazione di scelte tecnologiche volte a migliorare la sicurezza complessiva del cloud cifrato garantendo così la piena sicurezza dei dati in uso.
Nelle soluzioni ibride su licenza, inoltre, gli approfondimenti fatti dai rispettivi team di ingegneria hanno consentito di prendere delle decisioni architetturali volte non a massimizzare le soluzioni attualmente in commercio come Azure Stack Hub, ma a disegnare scenari più in linea con le soluzioni strategiche che daranno la massima applicazione nel prossimo futuro essendo basate su Azure HCI e Azure Arc.
La progettazione congiunta ha permesso di creare un sistema di governance del cloud cifrato che innalza la sicurezza complessiva, limitando le azioni possibili da parte della PA pur preservandone la flessibilità operativa, con un approccio secure by policy. Questa tipologia di governance consente di ridurre il personale del PSN dedicato al controllo della postura di sicurezza delle singole PA.
Infine, la partnership Leonardo – Microsoft, laddove applicata al PSN Cloud, consentirebbe di influenzare le roadmap di prodotto e assicurare la disponibilità delle nuove tecnologie richieste, temporalmente allineate quanto più possibile con le esigenze del mercato italiano.

Fondata nel 1975, Microsoft è tra le più grandi aziende di tecnologia al mondo ed è il più grande fornitore di hyperscale cloud aziendali al mondo. La sua offerta copre tutti e tre i livelli del cloud, IaaS, PaaS, SaaS con specifiche soluzioni, tra i leader di mercato e tecnologicamente molto avanzate, per il mondo ibrido.

La vasta gamma di servizi cloud di Microsoft è incentrata sulla sua tecnologia Azure per IaaS e PaaS. Oltre a questi elementi fondamentali, Microsoft ha esteso la gamma di prodotti Azure ad intelligenza artificiale, machine learning, IoT, sicurezza, database, gestione dei dati e altro ancora.

Microsoft Azure è costituito da oltre 60 Azure Region collegate dalla Microsoft Global Network. È una presenza capillare, guidata dalla intenzione di avvicinare le applicazioni agli utenti in tutto il mondo, mantenendo la residenza dei dati e garantendo scalabilità, conformità, sicurezza e resilienza.

Ogni Azure Region è costituita da un set di data center distribuiti entro un perimetro definito dalla latenza e connessi tramite una rete regionale dedicata a bassa latenza. Ognuno di questi set di DC forma una Availability Zone (zona di disponibilità), ovvero una località separata fisicamente all'interno della Region e totalmente indipendente. Le Availability Zone consentono di eseguire applicazioni mission-critical in *High Availability* dove si possono utilizzare repliche database e applicative sincrone a bassa latenza distribuite su un'area metropolitana. Per garantire resilienza ad un disastro grave che possa impattare tutte le Availiability Zone di un'intera Region, si può realizzare una soluzione di DR in una Region Azure secondaria nella stessa area geografica.

La Microsoft global network impiega oltre 130.000 miglia di fibra ottica e di sistemi di cavi sottomarini ed offre oltre 160 punti di presenza (edge locations) nel mondo. Il traffico IP rimane interamente all'interno della rete globale e non entra mai nella Internet pubblica. I clienti possono collegarsi alla global network con connettività dedicata Express Route fino a 100Gbps o in alternativa, in VPN.

Azure è un cloud hyperscale di successo, adottato da più del 95% delle aziende Fortune 500 in tutti i settori industriali.

Per i governi e il settore pubblico di tutto il mondo, Microsoft offre Azure, una piattaforma di servizi cloud multi-tenant pubblica e le tecnologie per realizzare una soluzione ibrida, che puoi usare per distribuire varie soluzioni in base al livello di controllo, di gestione e di rispetto di normative sulla residenza del dato. Una piattaforma di servizi cloud multi-tenant implica che più applicazioni e dati dei clienti siano archiviati sullo stesso hardware fisico.
Azure usa l'isolamento logico per separare le applicazioni e i dati di ogni cliente, offre meccanismi di crittografia e la possibilità di eseguire servizi su infrastrutture di ultima generazione che consentono di crittografare dati e programmi con chiavi possedute solo dal cliente finale (confidential computing). Questo approccio offre la scalabilità e i vantaggi economici dei servizi cloud multi-tenant, aiutando rigorosamente a impedire ad altri clienti di accedere ai tuoi dati o alle tue applicazioni.

Le tecnologie ibride di Microsoft estendono queste funzionalità e possibilità anche nelle infrastrutture on-premise. Utilizzando le funzionalità del cloud pubblico di Azure, in congiunzione con le sue soluzioni ibride, è possibile beneficiare della rapida crescita delle funzionalità, della resilienza e del funzionamento conveniente del cloud hyperscale, pur ottenendo i livelli di isolamento, sicurezza e affidabilità necessari per gestire i carichi di lavoro in un ampio spettro di classificazioni di dati.
Utilizzando le tecnologie di protezione dei dati di Azure e le funzionalità perimetrali intelligenti del portafoglio di prodotti ibridi, è possibile elaborare dati riservati in un'infrastruttura isolata e sicura all'interno del cloud pubblico multi-tenant o dati riservati in locale e all'Edge, con la piena operatività e controllo.

Microsoft Azure è particolarmente attenta in merito alla residenza dei dati e ai criteri di trasferimento. Microsoft Azure consente di specificare l'area di distribuzione dei servizi utilizzati e per questi servizi, Microsoft non memorizzerà i dati al di fuori dell'area geografica specificata.
E' possibile usare opzioni di crittografia dei dati complete e affidabili per proteggere i dati in Azure e controllare chi può accedervi.
Microsoft possiede oltre 90 certificazioni e investe ogni anno un miliardo di dollari in Cybersecurity per proteggere a ogni livello i servizi Cloud. La nuova Region Data Center italiana aiuterà ulteriormente le aziende ad adempiere al regolamento generale sulla protezione dei dati dell'Unione Europea (**GDPR**) e permetterà alle aziende di far risiedere i dati in territorio italiano.

1.7.3 Oracle Cloud

Partnership con Oracle
TIM, Oracle e Noovle (gruppo TIM) hanno firmato a luglio 2021 un Memorandum of Understanding (MoU) che definisce una partnership industriale fondata sui seguenti punti:

- utilizzo delle Soluzioni Oracle Cloud per gli ambienti della pubblica amministrazione e in particolare per il Polo Strategico Nazionale;
- ospitare una Region Italiana di Oracle nei Data Center di TIM;
- abilitazione di Noovle come Cloud Service Provider di Oracle.

Attraverso questo agreement TIM completa il piano di servizio Multi Cloud anche a livello di nodo di connettività e aggiunge ai precedenti accordi un tassello fondamentale per fornire ai clienti differenti opzioni di uso del cloud pubblico.
L'accordo con Oracle mira alla creazione di Soluzioni Cloud di tipo data-driven e abilita TIM-Noovle ad erogare servizi in ambito Cloud di Oracle includendo specificamente servizi basati su appliance ingegnerizzate (Exadata), il Cloud@Customer e la Region Dedicata.

Oracle Cloud Infrastructure (OCI) è una piattaforma ampia e profonda di servizi cloud pubblici che consente ai clienti di creare ed eseguire un'ampia gamma di applicazioni in un ambiente scalabile, sicuro, ad alta disponibilità e ad alte prestazioni.

Oracle Cloud Infrastructure combina l'elasticità del cloud pubblico con il controllo granulare, la sicurezza e la prevedibilità prestazionale di un'infrastruttura locale per offrire servizi di tipo enterprise (ad alte prestazioni, alta disponibilità) con costi contenuti.
Oracle Cloud Infrastructure offre servizi di infrastruttura (IaaS), di piattaforma (PaaS) e di servizi applicativi (SaaS) attraverso un insieme di "Region" distribuite nel mondo ed in continua espansione.

Le Region sono organizzate in uno o più Availability Domain (AD): Data Center vicini tra loro (area metropolitana), collegati da un backbone ad alta velocità, ma indipendenti.

All'interno di un Availability Domain le risorse fisiche (ad esempio i server) sono organizzate in tre Fault Domain (FD) distinti, per garantire adeguata protezione da hardware e power faults.

Molti servizi Cloud prevedono la replica automatica dei dati su storage server collocati in Fault Domain distinti, in modo da assicurare adeguata protezione dei dati e il cliente può scegliere la collocazione delle VM in Availability Domain e Fault Domain distinti.
Per soddisfare requisiti stringenti in termini di sicurezza, privacy, residenza e sovranità del dato, Oracle, in aggiunta alle regioni di tipo Public, offre il suo portfolio completo di servizi IaaS, PaaS e SaaS all'interno dei data center Private con la soluzione di Oracle Dedicated Region Cloud @Customer (DRCC). Ogni DRCC è composta da un Availability Domain e tre Fault domains.
Le Oracle Dedicated Region Cloud @Customer rappresentano un'area autonoma e disconnessa dalle Public Regions in cui tutti i dati, inclusi operations e metadati, rimangono locali nel data center.

Per la componente Oracle Database è possibile utilizzare i servizi nativi OCI Database Cloud Service che offrono la possibilità di istanziare ed usufruire di un database Oracle gestito in cloud con diverse opzioni possibili per meglio rispondere alle esigenze ed aspettative del cliente.

Tra le caratteristiche native principali dei servizi Oracle Database Cloud troviamo:

- Automazione per il provisioning di istanze di servizio Oracle Database tramite console, API, SDK, CLI;
- Supporto e certificazione per ambienti in configurazione cluster (attivo-attivo in lettura e scrittura) con Real Application Cluster;
- Supporto a deploy del servizio in ambiente virtualizzato, bare metal ed Exadata per garantire stessi livelli di scalabilità, performance ad affidabilità di quelli attualmente ottenuti on-premise;
- Automazioni native per backup, restore, patching, upgrade, cloning, scaling per una fornitura “DB as a Service” out-of-the-box;
- Gestione nativa dei PDB (Pluggable Database);
- Automazioni per Disaster Recovery tramite utilizzo di Data Guard con database primario e di standby su Region diverse;
- Monitoring integrato per le istanze Database;
- Piena compatibilità applicativa con le tecnologie Oracle Database utilizzate on-premise per una migrazione senza rischi;
- Cifratura di tutti i dati con controllo delle chiavi di cifratura;
- Utilizzo del modello pay-per-use e possibilità di utilizzo delle licenze Oracle in possesso tramite opzione BYOL (Bring Your Own License);
- Disponibilità della versione cloud Autonomous Database per un servizio completamente gestito (patching, backup, scaling etc..) e ottimizzato per carichi di lavoro di tipo Transazionale o Datawarehouse.

Oracle ha collaborato con enti di valutazione esterni e revisori indipendenti per soddisfare un'ampia serie di standard di conformità internazionali e specifici per l'implementazione di servizi Cloud, come ISO 27001, SOC1, SOC2, PCI DSS, HIPAA / HITECH e FedRAMP.
Oracle Cloud è inoltre un CSP (Cloud Service Provider) qualificato da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018.

Oracle Cloud Infrastructure è stato il primo cloud provider ad implementare una virtualizzazione di rete completamente isolata (definita "off-box" isolated network virtualization), che mantiene la virtualizzazione di rete e I/O isolata dall'hypervisor e quindi dalle Virtual Machine. Di conseguenza, i clienti possono eseguire in self-service il provisioning delle proprie risorse host (virtual machine o bare metal dedicati) garantendo il completo isolamento delle risorse e senza risentire del workload e del traffico generato dalle risorse assegnate ad altri clienti.

1.8 Certificazioni del Personale

Le singole aziende del costituendo RTI nell’ambito degli accordi di partnership, sopra citati, al fine di governare e gestire al meglio le tecnologie dei CSP, hanno avviato programmi di certificazioni del proprio personale. Tale programma proseguirà nel corso del 2022 ed al momento consente alla compagine di poter disporre di:

- > 1.250 certificazioni personali Google;
- > 300 certificazioni personali Microsoft;
- > 100 certificazioni personali Oracle.

L'eccellenza dei tre partner tecnologici si basa su personale altamente qualificato non solo per le soluzioni Hyperscaler, ma anche per le principali tecnologie leader di mercato che compongono tutta l'architettura necessaria a rendere fruibili e sicure le infrastrutture cloud. Si riportano, di seguito, le ulteriori principali certificazioni di cui si è in possesso a livello di architetture cloud:

- > 400 certificazioni personali VMware;
- > 50 certificazioni personali Red Hat;

e per le componenti di networking e sicurezza perimetrale:

- > 2.000 certificazioni personali Cisco;
- > 100 certificazioni personali Fortinet;
- > 80 certificazioni personali Palo Alto;
- > 85 certificazioni personali Juniper.

2 Servizi Offerti e Modalità di Erogazione

La PA potrà selezionare dal Catalogo un'ampia offerta di Servizi, con una proposta sempre allo stato dell'arte, aggiornata secondo le più avanzate tendenze del mercato e allineata alle innovazioni introdotte dagli *Hyperscaler*. L'erogazione dei Servizi richiesti sarà regolata tramite apposito contratto; la PA condividerà l'elenco aggiornato delle proprie dotazioni tecnologiche, e la NewCo PSN proporrà il servizio a catalogo che meglio copre l'esigenza della PA. Alla stipula del Contratto, sarà possibile procedere con le attività di Migrazione, propedeutiche alla fruizione del Servizio. **Il Contratto tra le PA e la NewCo PSN non sono oggetto del presente Progetto di fattibilità.**
I servizi offerti sono disponibili nelle seguenti modalità;

- Housing dedicato
- Hosting dedicato - con opzione su Rack dedicati e condivisi
- IaaS:
  - Private
  - Shared
- PaaS (DBaaS, PaaS IAM, Big Data, Artificial Intelligence)
- BaaS
- DraaS
- CaaS
- Security
- Public Cloud PSN Managed
- Secure Public Cloud
- Hybrid Cloud on PSN Site
- Multi Cloud
- Servizi di Migrazione, Evoluzione e Professional Services
- Business and Culture Enablement

L'infrastruttura sarà ospitata all'interno di **4 Data Center,** allestiti in **doppia Region (2 DC + 2 DC)** dotati di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire i massimi standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti.

2.1 Housing

Il **Servizio Infrastrutturale in modalità Housing Dedicato** consiste nella messa a disposizione, da parte della NewCo PSN, di aree **esclusive** all'interno dei Data Center, 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 nel ***capitolo 3 –***

Sicurezza *e* ***capitolo 4 - Infrastruttura IT e Network*** , atte ad ospitare le infrastrutture IT e TLC di proprietà delle PA, nonché di eventuali variazioni in corso d'opera.

2.2 Hosting

Il **Servizio Infrastrutturale in modalità Hosting Dedicato** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **fisica e dedicata**, in grado di ospitare tutte le applicazioni in carico alla PA 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 ***capitolo 3 – Sicurezza e capitolo 4 Infrastruttura IT e Network.***

Le modalità di erogazione del servizio sono due:

- Hosting dedicato su rack condivisi: le PA avranno accesso a infrastruttura dedicata all'interno di porzioni di rack, che saranno condivisi con altre PA.
- Hosting dedicato su rack privati: le PA avranno accesso a infrastruttura dedicata all'interno rack esclusivi / segregati.

La NewCo PSN sarà responsabile di tutti gli aspetti di gestione e manutenzione dell'infrastruttura hardware su cui è costruito il servizio.

2.3 IaaS

I servizi di tipo Infrastructure as a Service (IaaS) 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.

2.3.1 IaaS Private

Il **Servizio Infrastrutturale in modalità IaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **virtualizzata e dedicata**, in grado di ospitare tutte le applicazioni in carico alla PA 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 nel §. 4 Infrastruttura IT e Network.

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante e mettere a disposizione gli strumenti e le console per la gestione in autonomia degli ambienti fisici e virtuali contrattualizzati.

2.3.2 IaaS Shared

Il **Servizio Infrastrutturale in modalità IaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura **virtualizzata e condivisa**, in grado di ospitare tutte le applicazioni in carico alla PA 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 Infrastruttura IT e Network**.**

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

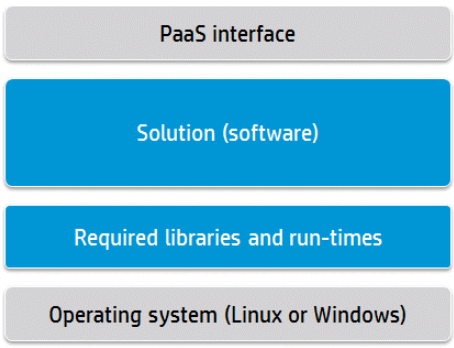
2.4 PaaS Industry

Il **Servizio PaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad esempio i Data Base, astraendo dall'infrastruttura sottostante.

La NewCo PSN, in qualità di provider, si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

L'offerta dei servizi PaaS prevede un approccio strutturato in cui ogni componente della soluzione PaaS, come il sistema operativo, solution stack ed altri software necessari, è strettamente controllato in termini di utilizzo e configurazione e gestito dal PSN. In questo caso le soluzioni vengono "create" al momento della necessità. Una rappresentazione di questa strutturazione vede quattro livelli di componenti:

- sistema operativo;
- run-time e librerie necessarie;
- soluzione caratterizzante – tipicamente un database, middleware, web server, ecc.;
- un'interfaccia programmatica con cui controllare gli aspetti operazionali della soluzione.



2.4.1 DBaaS

Il Database-as-a-Service è un servizio che consente agli utenti di configurare, gestire e ridimensionare database utilizzando un insieme comune di astrazioni secondo un modello unificato, senza dover conoscere o preoccuparsi delle esatte implementazioni per lo specifico database. Viene demandato al provider tutto quanto relativo all'esercizio e alla gestione dell'infrastruttura sottostante, comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche, mentre gli utenti possono così focalizzarsi sulle funzionalità applicative ed estrarre valore dai dati.

Tramite la console di gestione del servizio vengono messe a disposizione del cliente in particolare le funzionalità di:

- creazione (o cancellazione) di un database;
- modifica delle principali caratteristiche infrastrutturali dell'istanza DB e ridimensionamento ove non automatico;
- configurazione di alcuni parametri del database;
- attivazione di funzionalità aggiuntive, come ad esempio la replica dei dati su istanze passive (ove applicabile);
- attivazione di funzionalità di backup od esportazione dei dati (ove applicabile).

Altre funzionalità avanzate di configurazione delle specifiche istanze database sono demandate alle relative interfacce di amministrazione native.

Il catalogo del servizio comprende:

- **Database relazionali** (**Oracle DB Enterprise e Standard, MySQL, PostgreSQL, Maria DB, ...**) che supportano il modello dati relazionale e lo standard SQL di interrogazione. Sono quindi adatti a spostare carichi di lavoro di DB SQL preesistenti a casa del cliente su ambienti moderni e sicuri, in grado di garantire l'elevata affidabilità e le possibilità di crescita offerte dal Cloud.
- **Database NoSQL** (**MongoDB**, ...) ottimizzati per trattare dati non strutturati, con volumi elevati o con caricamento di grandi quantità di informazioni in modelli dati flessibili e con bassa latenza.

2.4.2 PaaS IAM

In aggiunta ai servizi di Identity and Access Management descritti al § 3.8.2che garantiscono i diritti di accesso alle componenti tecniche in ambito PSN (IaaS, PaaS, console unica di gestione, ecc.), viene reso disponibile dalla NewCo PSN un servizio di Identity Management applicativo che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano dentro il PSN.

Tale servizio ha lo scopo di integrare in modo facile e nativo le differenti esigenze di autenticazione e autorizzazione ad oggi previste all'interno del Codice dell'Amministrazione Digitale (CAD) ed in accordo con le normative vigenti in materia di trattamento dati riportate nel General Data Protection Regulation (GDPR).

Il servizio mette a disposizione le seguenti funzionalità:

- credenziali uniche di accesso alle applicazioni in perimetro e presidio efficace dei punti di accesso;
- implementazione di policy di cambio password, autenticazione a due fattori o semplicemente auditing e monitoring dei log di accesso;
- profilazione e segregazione delle informazioni in funzione dei propri privilegi: l'approccio di base si è concentra sulla creazione del "need-to-know". Le informazioni sensibili sono rese

disponibili solo a quelle persone dotate di adeguate autorizzazioni e di un "need-to-know" di tali informazioni per l'esercizio delle loro funzioni;

- controllo della diffusione delle informazioni: c'è una ragionevole probabilità che maggiori restrizioni sulla diffusione di informazioni sensibili riduce le possibilità di fughe di notizie e compromessi (“need-to-share”).

I principali moduli funzionali disponibili all’interno del servizio IAM fornito sono:

- **Identity Management & Governance**: è responsabile per la gestione del ciclo di vita delle identità digitali, gestisce la creazione, la modifica o la cancellazione delle identità, i loro attributi e il rapporto tra identità e attributi all'interno del sistema IAM. Inoltre, è responsabile per la gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestite le risorse di amministrazione;
- **Access Control & Management**: è responsabile di gestire l'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali;
- **Credential Management**: è responsabile per la gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.;
- **Multi Factor Authentication**: gestisce gli schemi di autenticazione utilizzati sul sistema IAM multifattore (gestione delle password, OTP Token, Smart Card, etc.). Per garantire la sicurezza dell’intera filiera applicativa il sistema di autenticazione multi-fattore deve garantire i livelli di sicurezza definiti all’interno della norma ISO/IEC DIS 29115
- **Logging & Reporting**: è il componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema IAM per generare rapporti per uso amministrativo o di revisione contabile;
- **Federation Services**: rappresentano i servizi di federazione verso Identity Provider Esterni garantendo la piena compatibilità con i più diffusi sistemi di autenticazioni federati (SPID, eIDAS, CNS, etc.). In particolare, con l’introduzione dello SPID (Sistema Pubblico di Identità Digitale) promosso dall’Agenzia per l’Italia Digitale (AgID), il servizio proposto consente di accedere con un unico login ai diversi servizi on line di tutti i Soggetti Pubblici (PA) e Privati che adottano questo sistema di autenticazione. Il servizio SPID Enabling consente di connettere e abilitare i servizi web di aziende pubbliche e private al sistema di autenticazione SPID (Sistema Pubblico delle Identità Digitali) basandosi su un gateway di federazione SAML 2.0 nel quale sono state implementate le logiche e le specifiche tecniche SPID ed abilita ad un sistema di autenticazione federato verso tutti gli Identity Provider accreditati AgID.

2.4.3 Big Data

Il servizio consente la costruzione di Data Lake as a service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale e un servizio per la data governance:

- **Data Lake**

Questa soluzione PaaS fornisce una piattaforma pronta all'uso che dispone di tutte le funzionalità necessarie a sviluppatori, Data Scientist e analisti per archiviare facilmente dati di tutte le dimensioni, forme e velocità.
Tale soluzione permette l'archiviazione e analisi di file con scalabilità orizzontale, lo sviluppo di programmi con architettura altamente parallela, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes), essere progettato per essere utilizzato su infrastrutture cloud e supportare una vasta gamma di linguaggi (Python,R, Java, .Net, Scala).

- **Batch/Real time Processing**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso per sviluppare processi batch e in streaming basati su un motore di esecuzione in Memory e basato su scalabilità orizzontale e parallela. Tale soluzione consente l'analisi di grandi moli di dati sia in batch che in streaming, un paradigma di programmazione unico per l'analisi in batch e in streaming, lo sviluppo di programmi performanti con utilizzo di architetture scalabili orizzontalmente e parallele, mette a disposizione Tool per il Debug e l'ottimizzazione dei programmi sviluppati, è Integrabile con Schedulatori di Risorse Esterni (YARN, Kubernetes) e cloud ready, supporta una vasta gamma di linguaggi (Python,R, Java, .Net, Scala), espone api rest per il monitoraggio e il submit dei job da remoto, fornisce un pannello per il monitoraggio del job e dettagli per singolo job, integrabile con Storage Esterni (Data Lake Paas), fornisce funzionalità di autoscaling e fornisce meccanismi di caching su SSD.

- **Event Message**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per sviluppare applicazioni e pipeline dati in real time inoltre deve fungere da Message Broker fornendo funzionalità di tipo Publish e Subscribe.
  Tale soluzione permette la gestione di grandi moli di eventi, lo sviluppo di programmi basati su architettura altamente parallela e scalabile orizzontalmente, fornire tool per il Debug e l'ottimizzazione dei programmi sviluppati, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes) e progettato per essere utilizzato su infrastrutture cloud, supportare una vasta gamma di linguaggi (Python, R, Java, .Net, Scala), fornire funzionalità di autoscaling, implementare meccanismi di consegna degli eventi in ordine ed essere integrabile con framework di Stream Processing (Spark).

- **Data Governance**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso che mette a disposizione un unico punto di riferimento sicuro e centralizzato per il controllo dei dati. Sfruttando strumenti di "search and discovery" e i connettori per estrarre metadati da qualsiasi sorgente di dati, permette di semplificare la protezione dei dati, l'esecuzione delle analisi e la gestione delle pipeline, oltre ad accelerare i processi ETL.
  Tale soluzione consente di analizzare, profilare, organizzare, collegare e arricchire automaticamente tutti i metadati, implementare algoritmi per l'estrazione di Metadati e relazioni in modo automatico, supportare il rispetto delle normative e della privacy dei dati con il tracciamento intelligente della provenienza dei dati (data lineage) e il monitoraggio della conformità, semplificare la ricerca e l'accesso ai dati e verificare la validità prima di condividerli con altri utenti, produzione di dati relativi alla qualità del dato, definire in modo semplice e veloce i modelli e le regole necessarie per validare i dati e risolvere gli errori,

permettere di supervisionare gli interventi per la risoluzione degli errori dei dati e mantenere la conformità rispetto a audit interni e normative esterne.

2.4.4 Artificial Intelligence

Il servizio mette a disposizione un set di algoritmi preaddestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning:

- **AI Platform**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per costruire modelli di ML/DL facilitando l'accesso al dato mettendo a disposizione una ambiente collaborativo a cui partecipano sia esperti di contesto che Data Scientist.
  Tale soluzione permette il supporto di almeno le seguenti tipologie di sorgenti dati: NoSQl, SQL, Hadoop File Formats, Remote Data Sources, Cloud Object Storage, Cluster Hadoop, Rest Api; fornisce moduli configurabili per il data cleaning, wrangling e mining, strumenti e librerie per la visualizzazione dei dati, supporta le principali librerie per lo sviluppo di modelli di ML/DK (PyTorch, TensorFlow, ScikitLeran, H20,XGBoost, etc), supportare gli ultimi trend tecnologici (AutoML, Explanable AI), supportare una vasta gamma di linguaggi (Python, R) e strumenti a Notebook (Jupyter), permette la gestione della sicurezza di livello enterprise con la possibilità di implementare politiche RBAC, fornisce un approccio visuale di tipo Drag&Drop per lo sviluppo, la gestione intera del ciclo di vita di un progetto di datascience (Business Undestanding, Data Acquisition&Understanding, Modeling, Deployment), rende possibile interrogare i modelli attraverso degli endpoint Rest, monitorare le performance dei singoli modelli, supporta sia CPU che GPU, permette il Deploy dei modelli in versione dockerizzata e su Kubernetes, permette la creazione di pipeline di automation per la creazione di ambienti e il rilascio dei modelli, permette la creazione di Wiki per la condivisione delle informazioni relative ai singoli progetti, è integrabile con IAM esterni, permette il tracciamento e monitoraggio di tutte le azioni effettuate sulla piattaforma, permette la gestione centralizzata delle risorse di computing, permette la possibilità di creare policy custom per la protezione del dato e integrabile con sistemi di calcolo distribuiti (Spark, Hive, Impala, etc).

- **Semantic Knowledge Search**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di rendere facilmente accessibili le informazioni contenute all'interno del patrimonio informativo (documenti, immagini, video) utilizzando un motore di ricerca semantico in grado di interpretare richieste in linguaggio naturale.
  Tale soluzione permette di gestire contenuti in varie tipologie di formati (Documenti Word, pdf, pptx , email, immagini, video, etc), di indicizzare le informazioni contenute nei documenti, l'implementazione di un motore di ricerca di tipo full-text e di tipo semantico performante, l'esposizione di un'interfaccia in linguaggio naturale, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo), implementare meccanismo di auto apprendimento mediante feedback utenti, garantire la sicurezza del dato con vari tipologie di protezione (At rest, In Transit), garantire scalabilità orizzontale, esporre delle api per l'integrazione con sistemi esterni e essere integrabile con uno IAM esterno.

- **Text Analytics /NLP**
  Questa soluzione PaaS rende disponibile una piattaforma pronta all'uso in grado di estrarre informazioni da testo non strutturato.
  Tale soluzione consente di esporre delle api rest per l'inferenza dei modelli, l'estrazione di Entità dal testo (Persone, Luoghi, etc), estrazione di concetti chiave dal testo, estrazione del Sentiment, riconoscimento della Lingua, garantisce scalabilità orizzontale, supporto Load Balancing, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo),il tracciamento e il monitoraggio delle interrogazioni al sistema e la possibilità di essere eseguibile su Kubernetes o in versione dockerizzata.

- **Audio Analytics**
  Questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti audio.
  Tale soluzione permette di analizzare grandi volumi di audio, garantire scalabilità orizzontale, supportare Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni da fonti audio (Analisi rumore ambientale, Speaker Identification, Audio Insight), esporre un'interfacciata basata su api rest per l'inferenza, permettere la configurazione degli algoritmi da User Interface, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generazione di Eventi verso sistemi esterni, elaborazione sia in streaming che in batch, algoritmi estendibili attraverso componenti dockerizzate e deployable su Cluster Kubernetes.

- **Video Analytics**
  Piattaforma PaaS pronta all'uso in grado di applicare algoritmi basati su AI su fonti video.
  Tale soluzione consente di analizzare grandi volumi di video, garantire scalabilità orizzontale, supporto al Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni dai video (Detection, Classification, Identification, Counting, Density Estimation), esporre un'interfacciata attraverso api rest per la lettura dei metadati generati dagli algoritmi, fornire un portale web per la configurazione dei flussi video e degli algoritmi, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generare Eventi verso sistemi esterni, elaborazione dei video sia in streaming che in batch e fornire estendibilità degli algoritmi attraverso componenti dockerizzate.

2.5 BaaS e DRaaS

Proteggere le applicazioni critiche facendo leva su un servizio di backup è allo stato attuale il modo migliore per garantire la continuità operativa. È fondamentale impostare per tutte le attività, anche e soprattutto quelle mission critical, un meccanismo automatico di duplicazione dei dati utilizzati e generati nelle attività quotidiane. Questo consente, in caso di interruzioni del servizio, attacchi informatici o perdita di informazioni, di accedere ai dati salvati e ripristinare immediatamente l'operatività di tutti i sistemi, riducendo al minimo – o addirittura azzerando – il downtime.

2.5.1 BaaS: Golden copy protetta

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard (cfr. § 4.1.5), la NewCo 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 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.

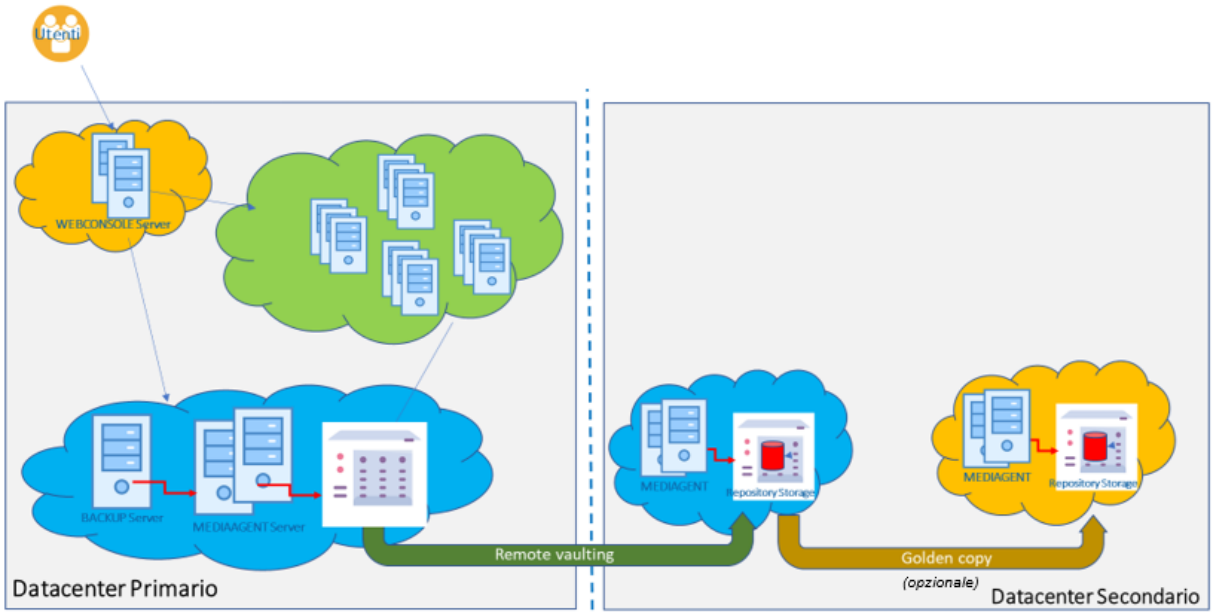


Figura 1: Architettura Funzionale Golden Copy

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 della NewCo PSN;
- ✓ protezione su storage distinto di backup, **privo di ogni accesso fisico e logico;**
- ✓ replica in **Region diverse e su canale cifrato**.

2.5.2 DRaaS

Il Disaster Recovery "*as-a-Service*" (DRaaS) è il servizio di cloud computing che consente il ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso. Il modello *as-a-service* prevede che l'amministrazione stessa non debba essere proprietaria di tutte le risorse né occuparsi di tutta la gestione per il Disaster Recovery, affidandosi al service provider per un servizio completamente gestito. La pianificazione del Disaster Recovery è fondamentale per la Business Continuity (cfr. "Specificazione caratteristiche del servizio e della gestione"). Il DRaaS si basa sulla replica e sull'hosting dei server in un site del PSN diverso rispetto all'ubicazione primaria. Il PSN implementa un piano di Disaster Recovery in caso di evento disastroso che causa l'indisponibilità del servizio un cliente.

2.6 CaaS

Il **Servizio Infrastrutturale in modalità CaaS** consiste nella messa a disposizione, da parte della NewCo PSN, di una infrastruttura in grado di distribuire e gestire tutte le applicazioni basate su **container** in carico alla PA 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. *Infrastruttura e Network.***

La NewCo PSN si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

2.7 Security

2.7.1 DDOS Protection

La NewCo PSN renderà disponibile per tutte le PA che attiveranno i propri servizi all'interno dell'infrastruttura proposta un servizio di Protezione DDOS. Tale servizio di Distributed Denial as a Service (DDoS) è un servizio di sicurezza infrastrutturale che va ad aggiungersi ed integrarsi ai servizi già previsti dal presente progetto.

Il servizio di DDoS Protection proposto dalla NewCo PSN garantisce la mitigazione degli attacchi DDoS provenienti esclusivamente da rete Internet e diretti ai sistemi delle Amministrazioni ubicati nei Centri Servizi previsti dal progetto.

La tipologia di attacco contrastata dal servizio offerto è il "Volumetric Attack" che mira alla saturazione del link di collegamento mediante la generazione di altissimi volumi di traffico e rendendo indisponibile il sistema del Cliente. Tale tipologia di attacco è generalmente generata da:

- botnet (reti di computer/server compromessi mediante malware e in possesso degli attaccanti),
- server in hosting con alta capacità di generazione traffico in banda,
- server/servizi che vengono abusati per generare traffico anomalo sfruttando debolezze dei protocolli esposti (DDoS Relection & Amplification),
- redirezione di traffico di navigazione da client leciti mediante compromissione di siti e banner pubblicitari,
- infrastrutture DDoSaaS (Distributed Denial of Service as a service anche dette Booter/Stresser) che consentono di lanciare attacchi di diversa tipologia previa pagamento di un abbonamento).

Il contrasto efficace di questo tipo di attacchi, per la loro stessa natura, può essere realizzato esclusivamente proteggendo le risorse trasmissive che forniscono la connettività Internet. Nel caso di attacchi DDoS la protezione risulta tanto più efficace quanto più è realizzata in prossimità delle sorgenti degli attacchi e quindi lontano dai target. Per tale motivo una protezione ottimale può essere realizzata solo ed esclusivamente nell'infrastruttura dell'operatore di TLC che fornisce il servizio di connettività.

Il servizio proposto è basato su una soluzione "surgical mitigation", ovvero una protezione che agisce esclusivamente sul traffico destinato al singolo IP attaccato e non su una soluzione "carrier agnostic", che per gestire una un attacco deve detenere completamente almeno una /24. La protezione "surgical mitigation" è sempre attiva ed efficace, mentre quella di tipo "carrier agnostic" risulta efficace solo in caso di attacchi realizzati puntando a risorse tramite un nome (FQDN - fully qualified domain name), sfruttando una redirezione basata su DNS non proteggendo nel caso di un attacco all'indirizzo IP assegnato alla risorsa.

Il servizio è applicabile esclusivamente alla connettività Internet condivisa fornita dalla NewCo PSN presso i propri Centri Servizi ed utilizzata dalle Amministrazioni che contrattualizzeranno i servizi infrastrutturali previsti dal presente progetto. Nello specifico il servizio DDoS Protection protegge esclusivamente IP pubblici esposti su Internet da attaccanti che siano in Internet, pertanto eventuali attacchi provenienti dalla rete INFRANET non sono né rilevabili né gestibili. Il servizio non è applicabile alla connettività INFRANET poiché quest'ultima è realizzata mediante una VPN MPLS.

Il servizio di DDoS Protection offerto prevede una gestione "proattiva automatica" con copertura H24. L'attività di contrasto ad un attacco di tipo DDoS è composta da tre fasi distinte:

- Diversion
- Cleaning
- Re-injection

La figura seguente mostra lo schema generico di funzionamento del servizio in caso di attacco.

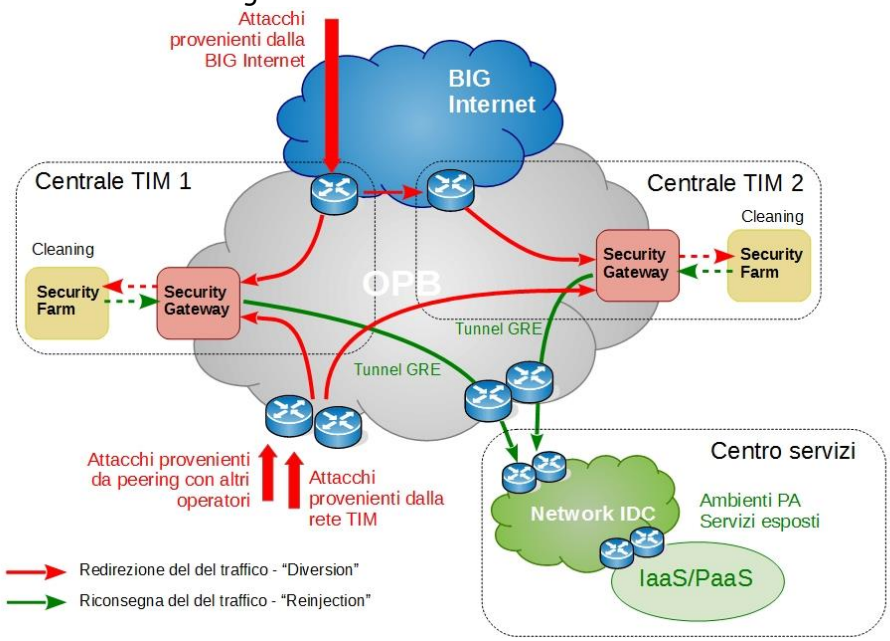


Figura 2: Rappresentazione dell'architettura di prevenzione del DDoS in presenza di attacchi

Di seguito sono dettagliate le tre fasi sopra indicate:

- Diversion: Il Security Operation center (SOC) attiva la redirezione del traffico Cliente riferito all'IP o agli IP sotto attacco verso le Security Farm con l'obiettivo di analizzare i flussi di traffico sotto attacco e intraprendere le azioni di cleaning.
- Cleaning: A seguito della diversion, il traffico è consegnato all'apparato di cleaning che analizzerà la tipologia dell'attacco e applicherà tutte le misure necessarie ad eliminare la sola componente indesiderata del traffico. Al termine delle attività di pulizia, il solo traffico legittimo è riconsegnato al Cliente attraverso la funzionalità di Re-Injection.
- Re-Injection: Il traffico legittimo viene riconsegnato al Cliente attraverso un tunnel GRE chiuso tra le Security Farm ed i router di attestazione del centro servizi che ospita i sistemi oggetto di attacco. Nello specifico il tunnel verrà chiuso sul router infrastrutturale del Centro Servizi presso cui sono posizionati i sistemi Cliente sul quale è terminata la connettività Internet. La modalità Tunnel GRE assicura che il traffico sia instradato in maniera puntuale.

2.7.2 Servizi Professionali di Sicurezza

Il PSN offre molteplici strumenti per gestire la sicurezza dei dati delle Amministrazioni e mitigare i rischi che tali dati vengano sottratti, rubati, modificati o distrutti. Rendere disponibili infrastrutture

intrinsecamente dotate di un livello di sicurezza elevato, di per sé non è sufficiente a garantire la completa sicurezza delle informazioni ivi trasferite. Questo principalmente per una serie di motivi tra cui:

- requisiti normativi cogenti di natura cyber/privacy;
- mancanza di flessibilità nella stipula dei contratti;
- mancanza attuale di pubblicazioni o risposte in merito alla conformità a standard applicabili per la normativa italiana;
- scarsa conoscenza della nuova tecnologia e conseguente sottovalutazione dei rischi di migrazione;
- necessità di ridisegnare le architetture e i controlli di sicurezza, in quanto quelli utilizzati in ambienti tradizionali spesso non risultano efficaci in ambienti cloud o multicloud;
- difficoltà e complessità a mantenere centralizzato il governo dei processi e le tecnologie di sicurezza, anche e soprattutto in scenari multicloud ibridi;
- poca conoscenza e conseguente difficoltà ad abilitare e sfruttare i seppur efficaci strumenti di sicurezza nativi dei cloud provider;
- difficoltà di gestire i processi di audit e gestione degli incidenti, soprattutto in casi di analisi post-mortem e forense.

In conseguenza di tutte le problematiche sopra evidenziate vengono proposti servizi professionali per affiancare le Amministrazioni nell'implementare le opportune contromisure all'interno del proprio ambiente cloud.

2.7.2.1 *Ambito di attività*

I servizi professionali relativi agli ambiti di sicurezza erogati dal PSN saranno a disposizione delle Amministrazioni per tutte quelle attività necessarie ad aumentare il livello di sicurezza e a mitigare i rischi, tra cui:

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

Durante la fase di migrazione, sulla base del livello di sicurezza richiesto e della sensibilità dei dati migrati, i servizi professionali potranno fornire il supporto necessario all'implementazione dei controlli, allo scopo di attivare i servizi richiesti dalla PA, tra cui:

- cifratura dei dati “In motion” (traffico di rete di risorse esposte e non esposte) e “At rest”;
- gestione delle chiavi di cifratura;
- definizione di policy per il controllo degli accessi per tutte le tipologie di utenze degli ambienti cloud (applicative, nominali, amministrative) secondo il principio del “Least Privilege”;
- valutazione e configurazione di Password Policy;
- rilevazione continua delle configurazioni di “default”;
- rilevazione e monitoraggio continuo degli accessi alle risorse cloud e delle chiavi di accesso;
- adozione di utilizzo di tecniche di autenticazione a 2 fattori (2fa) e di meccanismi di Single Sign On (SSO);
- messa in sicurezza degli endpoint (Antimalware, HIPS, Data Loss Prevention);
- centralizzazione degli eventi di sicurezza e log e correlazione degli eventi;
- verifica del livello di logging delle applicazioni e implementazione del livello adeguato alle attività di monitoraggio, gestione incidenti e auditing;
- accesso sicuro agli ambienti Cloud tramite link dedicati e/o Virtual Network.;
- hardening dei sistemi IaaS e PaaS.

Inoltre, potranno essere richieste le seguenti attività aggiuntive:

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

I servizi sopra elencati forniranno un ulteriore livello di sicurezza, rispetto agli standard di sicurezza adottati nel perimetro del PSN descritti al paragrafo 3, che potranno essere attivati su richiesta della singola PA. L’obiettivo di tali attività è identificare, classificare e mitigare i rischi e le vulnerabilità all’interno del perimetro di servizio della singola Amministrazione.

Per ogni progetto verrà individuata il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste.

2.8 Refresh tecnologico

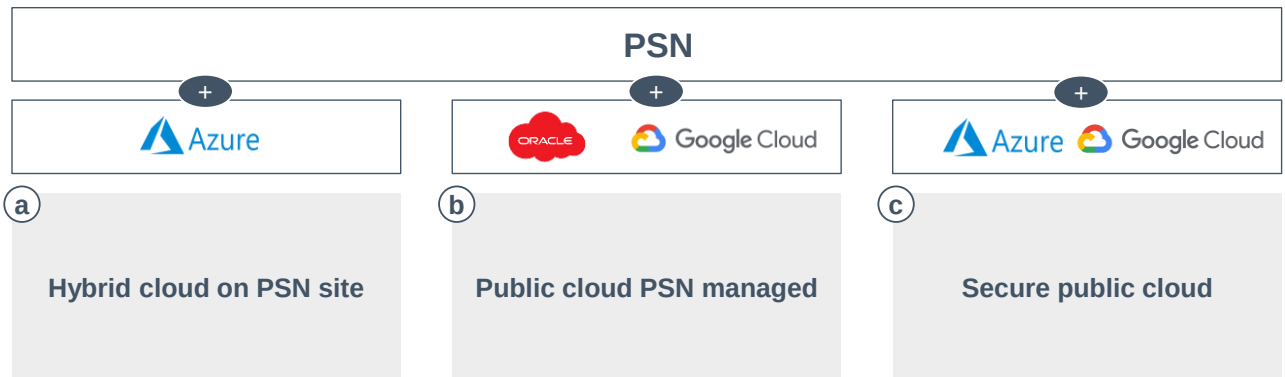
Di seguito la descrizione della modalità di gestione del refresh tecnologico.
L’architettura Cloud è basata sulla integrazione tecnologica di componenti HW e SW che hanno un determinato ciclo di vita garantito dalle roadmap dei diversi HW/SW Vendor. Partendo da

questo presupposto, si prevede per l'architettura Cloud (incluso il servizio di Hosting) un ciclo di vita di circa 5 anni relativamente alle componenti HW (fondamentalmente computing layer).
A fronte di una dichiarazione di End of Support/Life dallo specifico HW Vendor, si procederà alla valutazione delle componenti di nuova generazione da integrare nell'architettura, all'integrazione nel perimetro di servizio e alla successiva sostituzione di quelle in servizio.
Dal punto di vista del SW, invece, il processo prevede il mantenimento dello stato dell'arte attraverso l'implementazione degli aggiornamenti forniti dai relativi SW Vendor, seguendo le procedure che saranno definite dalla NewCo PSN che permetteranno di mantenere la continuità di servizio.
In caso di annuncio di End of Support/Life per un prodotto, si procederà all'analisi e allo studio di fattibilità per giungere alla implementazione di una nuova versione SW. Tale attività prevede anche la validazione da parte della funzione Security al fine di garantire il più alto livello di sicurezza che sarà garantito dalla NewCo PSN.
Tali aggiornamenti, soprattutto quelli SW, trattandosi di attività che riguardano il livello infrastrutturale della piattaforma Cloud sottesa all'erogazione del servizio per le PA, potrebbero avere degli impatti sulle VM/Applicazioni della PA e quindi, in ogni caso, ogni singolo refresh tecnologico, HW o SW che sia, verrà verificato con i referenti della PA qualora comportasse necessari requisiti anche lato VM/Applicazioni e quindi potenziali modifiche preventive da parte del cliente finale.

2.9 Il ruolo dei CSP

La NewCo PSN, oltre a rendere disponibili servizi Cloud che erogherà da un'infrastruttura realizzata appositamente per il seguente progetto, offrirà ulteriori servizi cloud avvalendosi della collaborazione dei principali Cloud Service Provider (CSP).

La PA tramite il PSN potrà accedere in piena sicurezza e sovranità ai servizi dei CSP in funzione dei suoi bisogni e in modalità Private, Hybrid e Public.



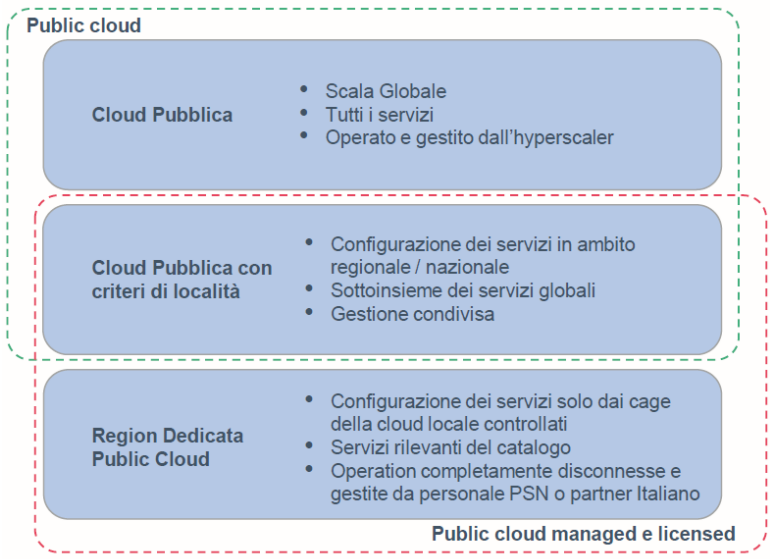
Nello specifico i servizi che verranno descritti nei successivi paragrafi vedono il coinvolgimento di Google, Microsoft ed Oracle.

2.9.1 Public Cloud PSN Managed

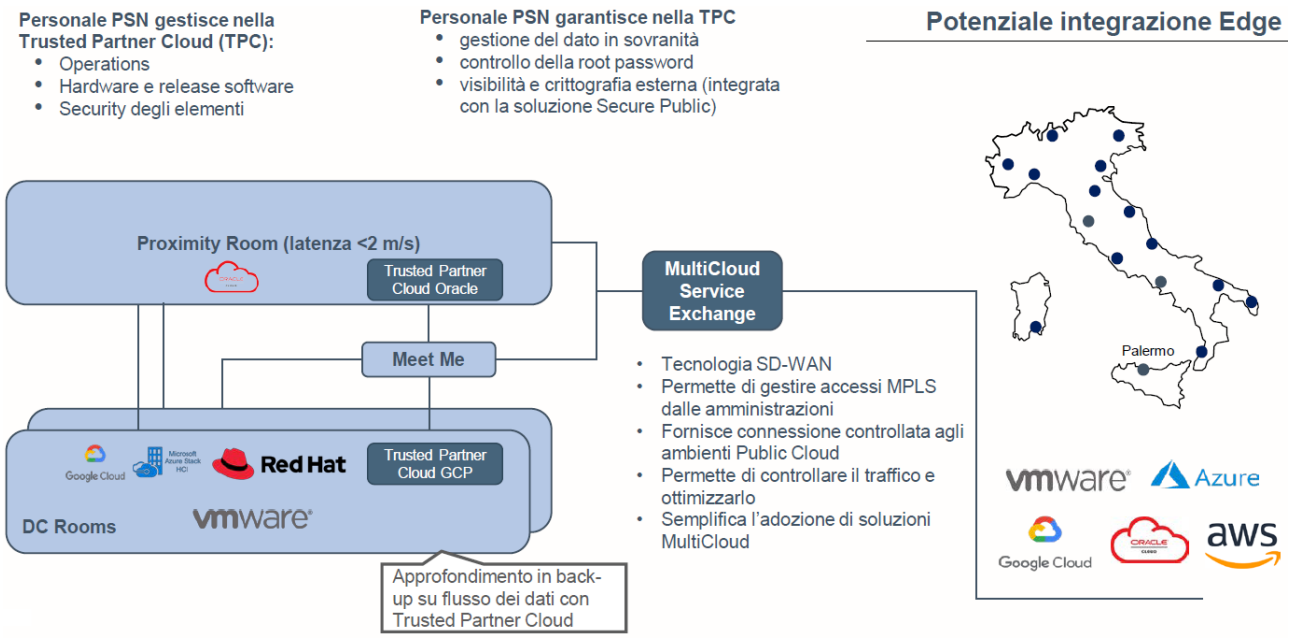
A seguire un overview sul Public Cloud PSN Managed i cui dettagli sono descritti nel proseguio del paragrafo.

Il Public Cloud PSN Managed permetterà alle PA di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica e gestione operata da personale PSN.

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



- **Partner di fiducia**: TIM partner italiano, formato su tecnologia di base GCP e Oracle
- **Ispezione dei controlli:** personale PSN e/o di TIM ispeziona l'implementazione e il funzionamento dei controlli di Google e Oracle. Ciò include audit del codice, l'accesso alla telemetria di sicurezza e strumenti per applicare e monitorare l'implementazione dei controlli dei propri clienti su Google Cloud
- **Approvazione del Partner**: alcune classi di accesso amministrativo ai dati, implementazioni di sistemi critici, deploy e modifiche del codice, modifiche operative richiederanno un LGTM esplicito da parte del partner per il completamento
- **Root of Trust esterna:** il partner controlla la root of trust per tutti i dati dei clienti. In caso di comportamento reputato non appropriato da parte degli hyperscaler (Google e Oracle), il partner potrà revocare l'accesso alla gestione delle infrastrutture



Il Servizio di Public Cloud PSN Managed è basato sulle tecnologie e i 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 della NewCo PSN o dei 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 e gestita totalmente da personale della NewCo 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 la NewCo 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.

2.9.1.1 *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 disporrà di istanze del cloud Hyperscaler aggiungendo i propri domini, indirizzi IP, branding, fatturazione e sarà 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 Public Cloud PSN Managed sono i seguenti:

- Fornitore dei servizi Cloud (CSP) che dedicherà 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);
- Provider di servizi PSN (MSP-PSN).

L'MSP sarà responsabile end-to-end della gestione operativa della Region dedicata; avrà 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 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.

2.9.1.2 *Architettura fisica*

Il Public Cloud PSN Managed sarà implementato all'interno di una delle *Region* del PSN, prevenendo 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. Ognuna delle Region dovrà avere almeno 3 high availability zone.

Nelle zone il CSP individuerà delle aree per isolare fisicamente gli apparati dedicati al PSN, e l'MSP avra' 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 (accesso *escorted*).
Sarà possibile per l'MSP anche ispezionare gli strumenti e le apparecchiature usate per gli interventi.

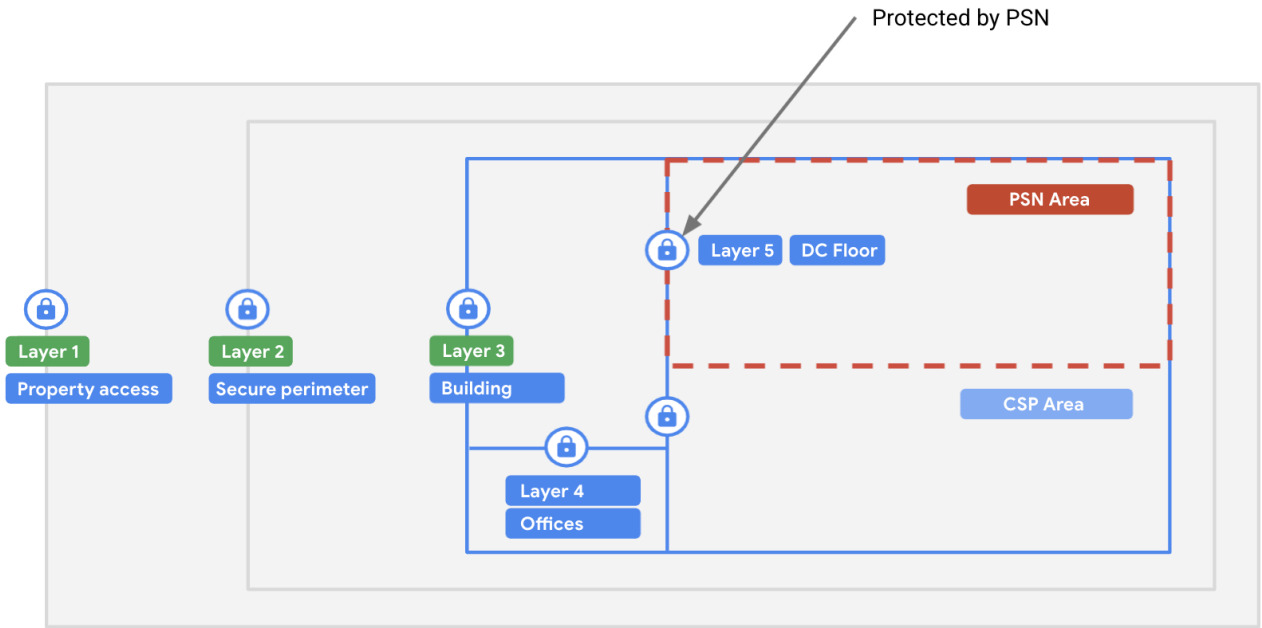


Figura 3: Livelli di segregazione

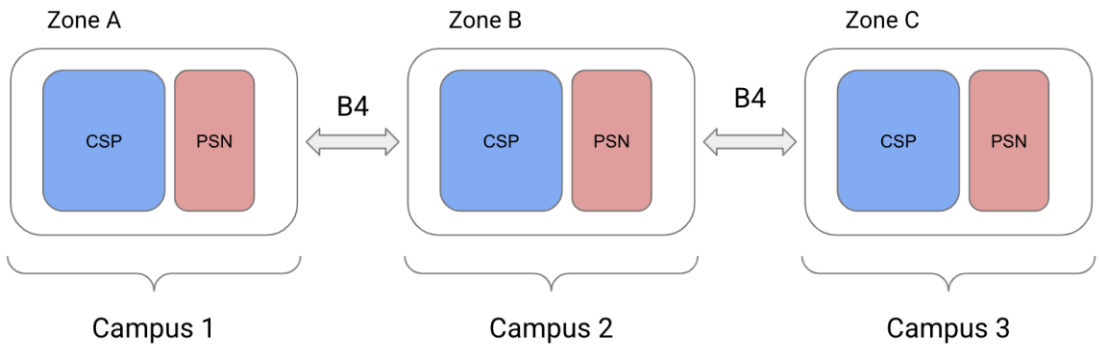


Figura 4: Isolamento fisico delle aree dedicate al PSN

2.9.1.3 *Ripartizione delle responsabilità*

Il modello Public Cloud PSN Managed prevede una ripartizione delle responsabilità che lascia all'MSP il pieno controllo dei *layer che vanno dalla gestione logica della rete fino alla sicurezza applicativa*.
Il CSP avrà 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 la possibilità' di fare code *inspections* e la review delle modifiche.

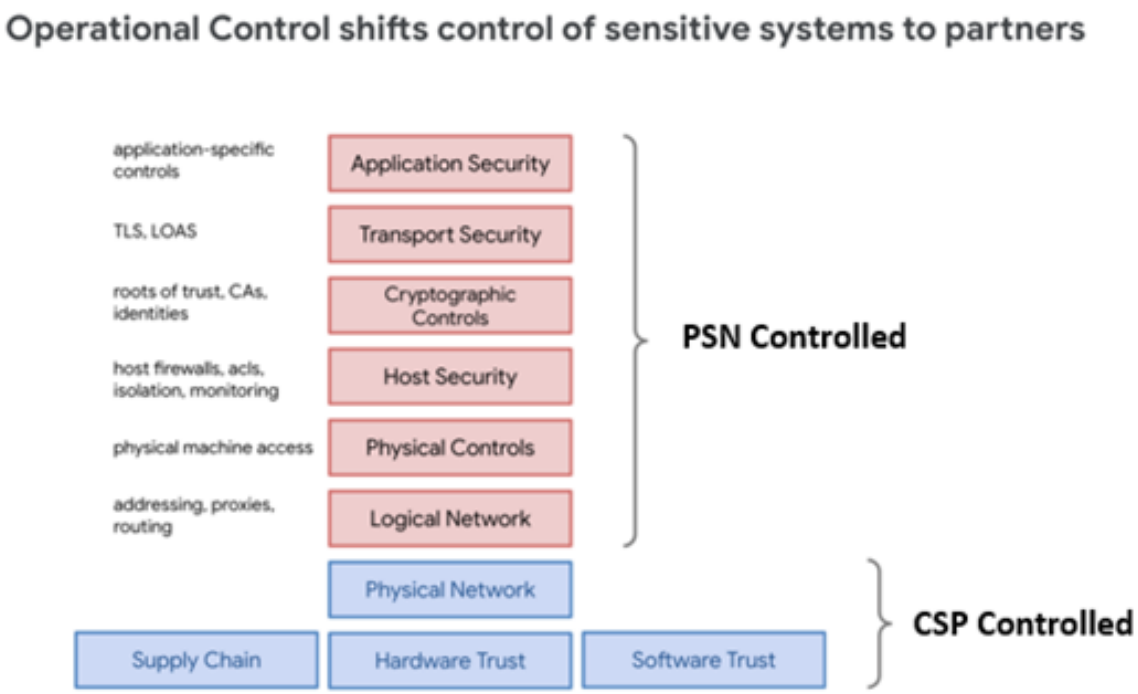


Figura 5: Distribuzione dei livelli di Operational Control per il Public Cloud PSN Managed

2.9.1.4 *Controllo della Rete*

L'MSP 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 riguarderà 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.

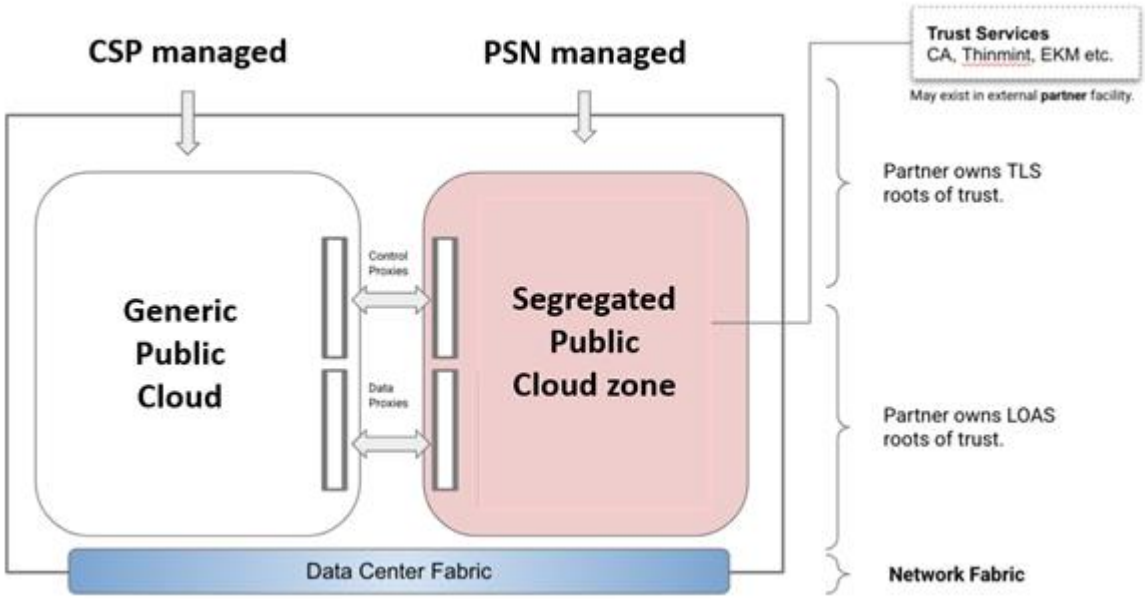


Figura 6: Aree di intervento del PSN per il Public Cloud PSN Managed

2.9.1.5 *Accesso verso l'esterno Frontend*

L'MSP 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 potrà disporre anche di propri DNS, load balancer, VIP tunneling e strumenti di gestione aggiuntivi.
Rientra inoltre sotto il controllo dell'MSP anche tutta la gestione delle *key chains*: nomi di dominio, certificati TLS, CA, rotazione delle chiavi, scadenza, ecc.

2.9.1.6 *Encryption at-rest*

Tutti i dati verranno cifrati in modo trasparente *at-rested in-transit*. Le chiavi di cifratura saranno custodite dall'MSP 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 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 dovranno essere cifrati con questo meccanismo. Sarà cura dell'MSP custodire le chiavi garantendo l'alta disponibilità' e la protezione da eventuali eventi di disastro, per scongiurare l'impossibilità di poter decifrare i dati.

2.9.1.7 *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 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.
Un possibile meccanismo a tutela di ciò' è il seguente:

1. Il CSP pubblica dei file binari (firmati digitalmente) su un repository protetto accessibile in modo esclusivo da parte dell'MSP. Il MSP avrà modo di analizzare i sorgenti con cui sono state eseguite le build e con cui sono stati rilasciati i relativi moduli.
2. Dopo un periodo di tempo concordato, il CSP rilascia i nuovi moduli su un'ambiente isolato all'interno della Region e accessibile solo al personale preposto alle verifiche dell'MSP.
3. Il MSP esegue tutti i test di sicurezza sull'ambiente "in quarantena", analizzando ad esempio il traffico di rete per individuare eventuali anomalie e flussi inattesi o sospetti.
4. A valle delle verifiche, il MSP firma i binari con un proprio certificato e approva il deployment.
5. Viene effettuato infine il deployment su ambiente di staging per ulteriori test e dopo un periodo di collaudo avviene il rilascio finale in produzione (se non vengono evidenziate anomalie)

2.9.1.8 *Modello di Supporto*

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

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

2.9.2 Secure Public Cloud

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

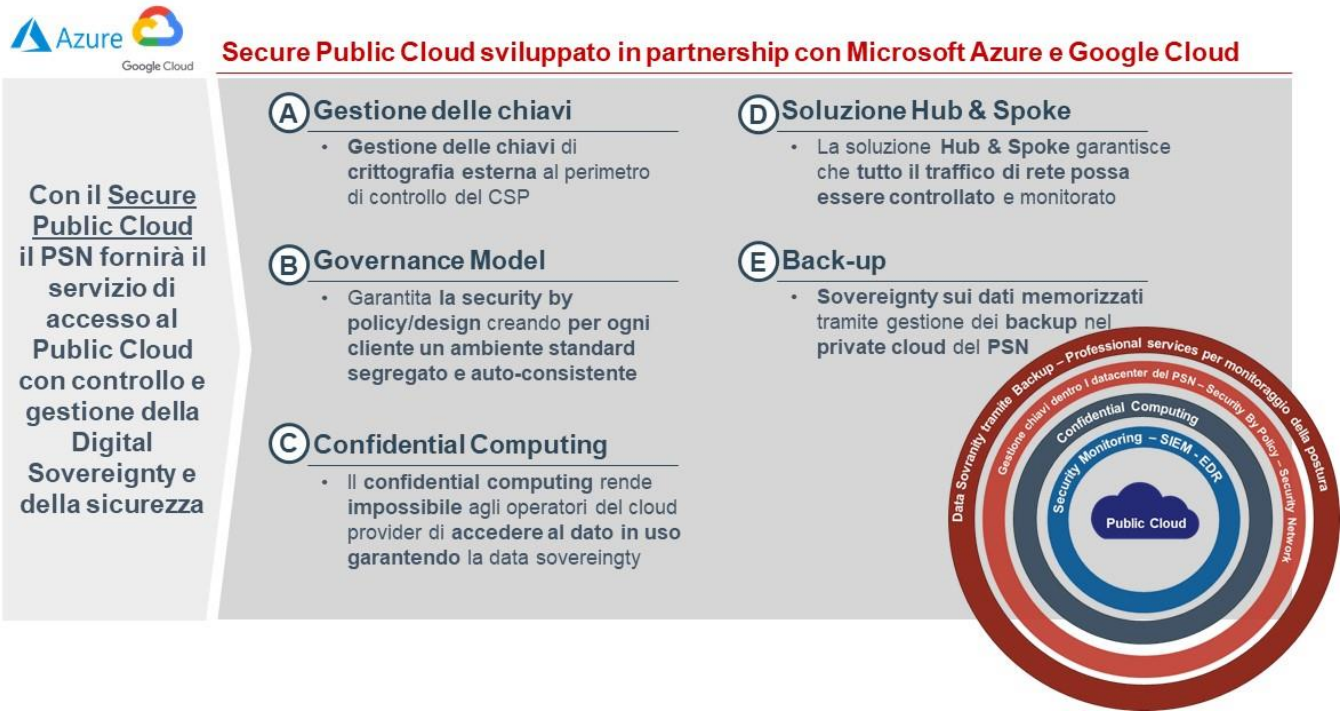
- **Public Cloud:** La componente **Hyperscale Public Cloud,** erogata da una *Region* collocata sul territorio nazionale, ai cui servizi vengono applicate configurazioni, policy e controlli di sicurezza, al fine di garantire ai clienti ambienti di elaborazione segregati aventi una sicurezza di base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

- **Security & Governance**: Una componente, erogata dal 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.

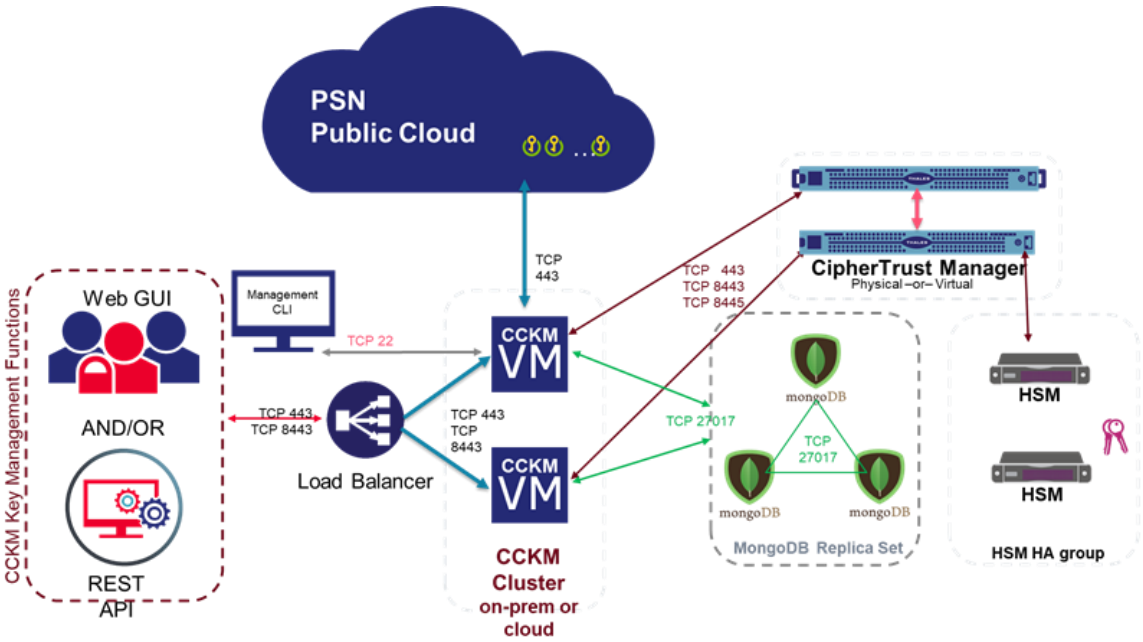
Il Secure Public Cloud è un servizio core del PSN che garantisce alti standard di sicurezza.



A. GESTIONE DELLE CHIAVI. Relativamente alla gestione delle chiavi la proposta 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.

B. **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:

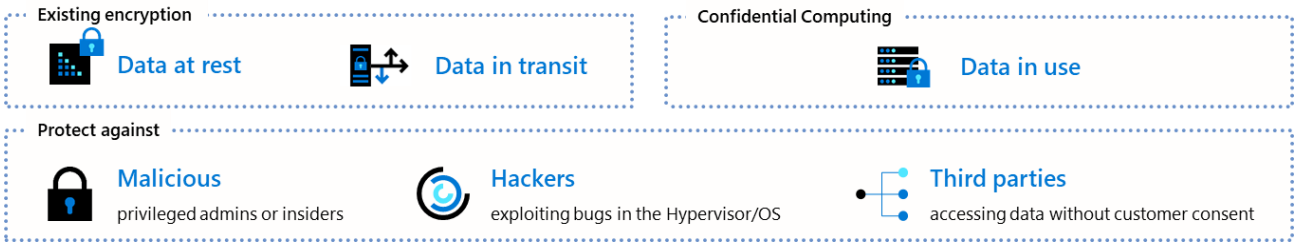
- Gestione uniforme e standardizzata dei tenant cliente;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, di set di regole di sicurezza predefinite in linea con best practices internazionali;

- 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;

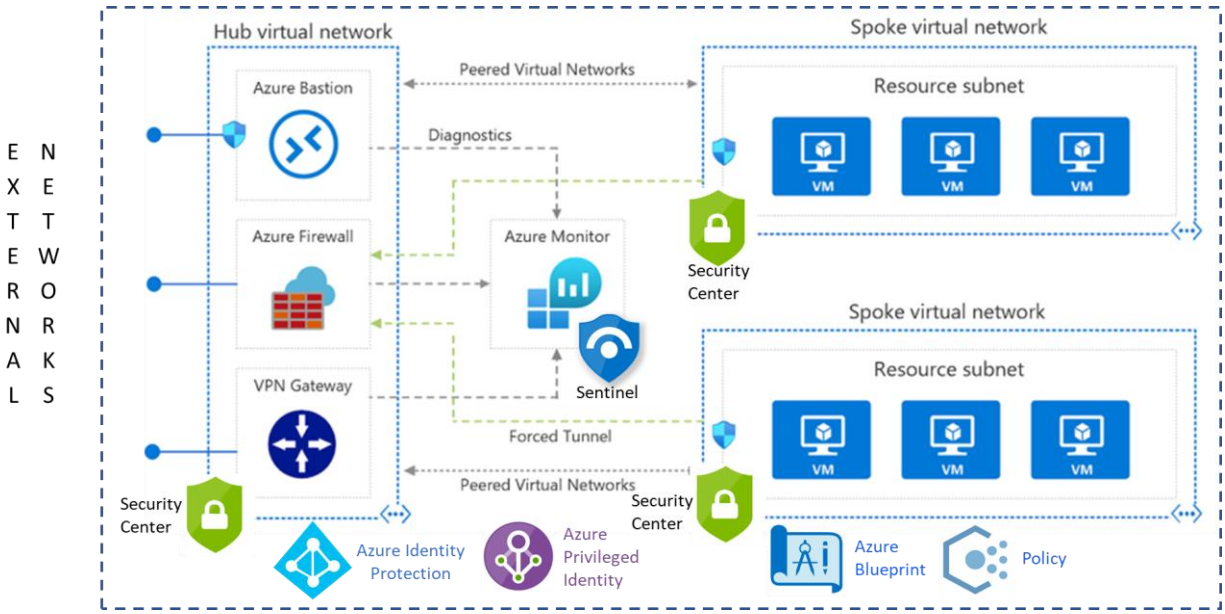
C. **CONFIDENTIAL COMPUTING.** L'obiettivo del PSN è rafforzare il livello di confidenzialità e sicurezza del dato in uso tramite i seguenti metodi:
   - Ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations.
   - Usare tecniche di enforcement basate su 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.

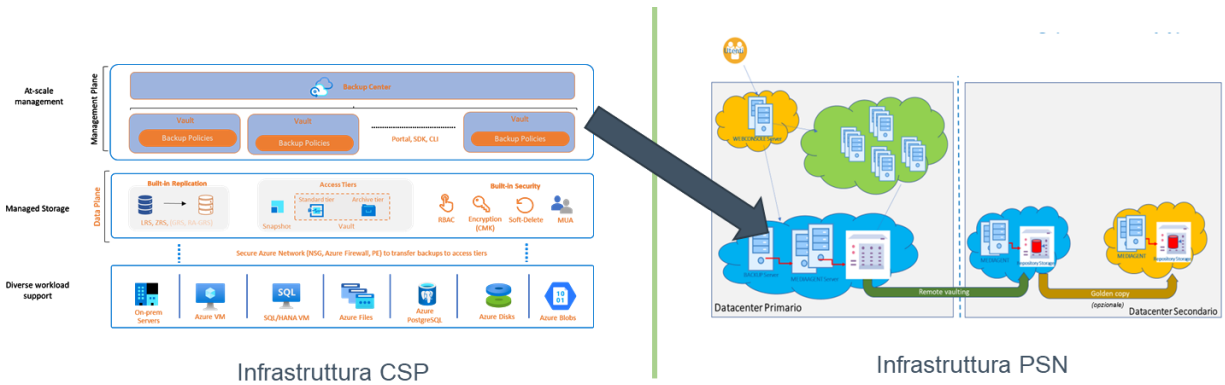
Confidential Computing (per VM, K8S, HSM) è la protezione dei dati in uso utilizzando ambienti di esecuzione attendibili basati su hardware



D. **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.



E. 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-as-a-Service 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.



2.9.2.1 *Requisiti architetturali*

Per l'erogazione del servizio, devono essere soddisfatti i seguenti requisiti architetturali:

- **Il PSN è il fornitore di piattaforma**: il ruolo principale è garantire che le componenti su cui si basano i servizi offerti rispettino costantemente i requisiti di sicurezza di base. A tale fine, deve venir applicato un approccio di "visibilità" centralizzata, controllo dei servizi di sicurezza, e deployment distribuito, occupandosi di:

- definire uno specifico catalogo di servizi utilizzabili dalla PA all'interno del perimetro del Secure Public Cloud;
- definire i modelli/template degli ambienti che i clienti possono istanziare e garantirne l'*enforcement* delle configurazioni;
- implementare e controllare negli ambienti dei clienti le risorse che compongono i servizi di sicurezza di base e le policy/regole definite per la compliance degli ambienti;
- controllare la persistenza delle configurazioni e la postura di sicurezza di tutti i servizi Public Cloud del PSN.

- **Governance gestita via Policy**: gli ambiti di gestione dei vari attori sono definiti sotto forma di *Policy*, per garantire la conformità continua della piattaforma alle regole di sicurezza richieste dal PSN. Allo stesso tempo, le *Policy* consentono ai gestori sia un adeguato grado di libertà che un percorso controllato nell'adozione del modello Cloud. La governance degli ambienti deve definire regole codificate non aggirabili e/o sottoponibili a auditing per la verifica e successivo adeguamento, per creare dei confini autoritativi su tutta la piattaforma. In sintesi, le Policy garantiscono la compliance alle regole del PSN.
- **Democratizzazione degli ambiti di gestione:** il disegno non deve prevedere la centralizzazione del controllo sulle operazioni di creazione degli ambienti o delle risorse. La collocazione degli ambienti e delle risorse all'interno degli ambiti di applicazione delle policy deve garantire l'applicazione automatica delle salvaguardie native del PSN, grazie alla natura "ereditaria" delle Policy. Questo consente un ampio uso delle modalità self-service, pur mantenendo il controllo della sicurezza.
- **Change Control**: monitoraggio continuo della postura di sicurezza della PA attraverso sistemi di automazione e orchestrazione con l'obiettivo di identificare ed evidenziare modifiche che possano avere un impatto sulla sicurezza della PA, ai quali verranno sottoposte per verifica ed eventuale adeguamento.
- **Difesa in profondità:** applicando una logica a più livelli al controllo delle risorse in un sistema è possibile ridurre la probabilità che un attacco abbia successo. Infatti, un approccio al controllo delle risorse fatto a più livelli, costringe gli utenti non autorizzati ad impegnarsi per aggirare ciascun controllo, prima di poter accedere a una risorsa.
- **Verifica esplicita**: qualsiasi operazione di autenticazione o autorizzazione nella piattaforma deve validare i *data point* disponibili, quali identità dell'utente, posizione, integrità del dispositivo, servizio o applicazione, classificazione dei dati e anomalie.
- ***Least Privilege*:** l'architettura consente, in ogni sua componente, la gestione delle risorse senza l'utilizzo di privilegi persistenti, e di governare l'accesso degli utenti in modalità *just-in-time* e *just-enough-access* (JIT/JEA), nonché di attuare politiche di enforcement adattative basate sulla valutazione del rischio, al fine di garantire sia la produttività che la protezione dei dati.
- ***Assume Breach***: al fine di minimizzare gli impatti di eventuali compromissioni, occorre mantenere strettamente segregati gli ambienti dei clienti, usare servizi di cifratura del dato

e delle trasmissioni per default, e utilizzare *analytics* per ottenere visibilità e capacità di *detection* rapida e incrementare le difese e le capacità di risposta.

- ***Data sovereignty***: al fine di garantire la conservazione dei dati occorre mantenere le copie di backup delle infrastrutture e dei dati sia all'interno dello spazio dell'Hyperscaler sia conservarle all'interno dei Data Center del PSN.

2.9.2.2 Architettura

L'architettura prevede due componenti primarie:

- **Servizi "Public Cloud"**: il disegno prevede l'uso dei servizi di un CSP presso cui creare un ambiente (*Tenant-Cloud*) per ciascun cliente ed uno dedicato al PSN. All'interno di ciascun *Tenant-Cloud* dei clienti finali sarà definita un'architettura a "segmenti" a cui saranno applicate *Policy* coerenti con il tipo di applicazioni che il segmento deve ospitare. La gestione operativa di questi segmenti sarà delegata con una logica di tipo RBAC, che consente la definizione di un modello i cui ruoli potranno essere assegnati al cliente finale. Sarà definito anche un segmento "speciale" (*Core*) in cui saranno attivate le risorse necessarie al controllo e all'enforcement della postura di sicurezza del cliente, il cui controllo sarà appannaggio del MSP-PSN. Come detto, su tutti i segmenti, e a diversi livelli, saranno applicate le *Policy* che garantiscono la coerenza del PSN con il modello di sicurezza richiesto per tutte le risorse definite, indipendentemente dai tempi di deployment.
  Si prevedono come necessari le seguenti componenti:

  - ***Confidential Computing:*** L'uso dei servizi del Secure Public Cloud richiederà la cifratura del dato e del traffico per default. Per applicazioni che gestiscono dati è necessario avere un controllo più stringente della catena di *trust* ed occorrerà usare meccanismi di cifratura cosiddetti "*in use*", quali il *Confidential Computing*. Il servizio di Secure Public Cloud deve essere fornito da Data Center realizzati sul territorio Nazionale.
  - ***Cifratura e gestione delle Chiavi:*** le regole del PSN richiedono la cifratura dei dati at-rest e in-flight, sia per applicazioni "convenzionali" che per quelle che richiedono controlli più stringenti; si farà quindi uso di servizi di Key Management presenti nell'ambiente Cloud che consentiranno la gestione del ciclo di vita delle chiavi in maniera integrata con l'analogo servizio implementato On-premise dell'infrastruttura descritto al punto successivo.
  - **Architettura Logica Hub&Spoke**: Per quanto riguarda l'ambiente 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.

- **Security & Governance:** l'architettura prevede la realizzazione di ambienti di erogazione di servizi presso i Data Center del PSN, che implementino servizi atti ad aumentare la sicurezza del Public Cloud, quali:

- servizi di **Key Management** tramite appliance HSM gestite, con l'obiettivo di sfruttare meccanismi di *Bring Your Own Key* (BYOK) sul Public Cloud, garantendo la proprietà e la completa gestione del ciclo di vita delle chiavi di cifratura in ambiente protetto e dedicato;
- servizi di **Backup** allo scopo di realizzare una seconda copia dei dati conservata all'interno del PSN e al di fuori del controllo del CSP, per assicurare in ogni momento il mantenimento della sovranità del dato;
- servizi professionali opzionali di gestione della sicurezza per monitorare continuamente le Security Posture dei Tenant su Public Cloud.

2.9.2.2.1 Cifratura e gestione delle chiavi (Key Management)

Vista la natura di sicurezza dei servizi del PSN, le capacità di crittografia della piattaforma sono fondamentali, in quanto non proteggono semplicemente il dato, ma, soprattutto, grazie al controllo all'accesso, sono il modo più efficace per esercitare il controllo sulla sovranità. È previsto che la piattaforma PSN fornisca servizi di crittografia e gestione delle chiavi e il servizio di *Key Management* deve essere basato su apparati HSM certificati FIPS 140-2 Level 3.
Di seguito la lista delle caratteristiche previste dall'architettura per il servizio:

- **Ambiente Public Cloud**:
  - È previsto l'uso dei servizi di gestione delle chiavi native, poiché questi sono integrati con la piattaforma. In questo modo i clienti saranno in grado di utilizzare un ampio spettro di servizi IaaS e PaaS mantenendo un forte controllo sull'accesso ai loro dati e alle loro chiavi. Per ottenere un controllo più stringente l'architettura prevede che ci sia la possibilità di gestire il ciclo di vita delle chiavi al di fuori del servizio di Key Management istanziato su Public Cloud (in particolare sarà possibile farlo con l'omologo servizio On-premise), e importare le chiavi all'interno del servizio Cloud, usando protocolli standard definiti allo scopo.

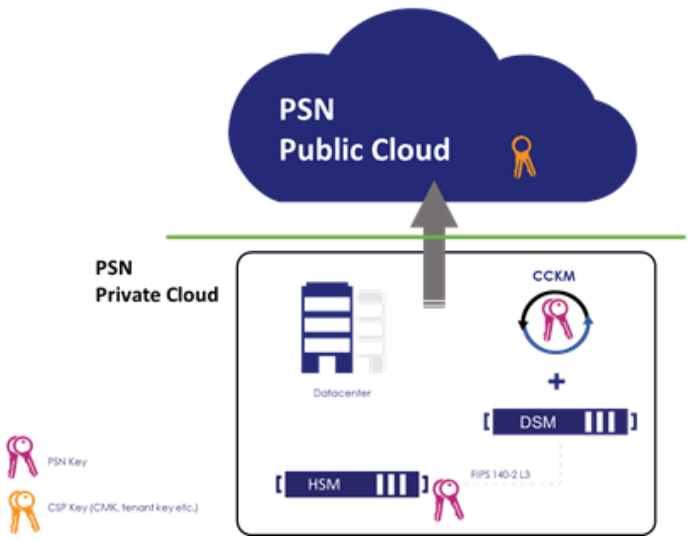


Figura 7: Architettura Secure Cloud Service

L'architettura prevede che il servizio di Key Management sia implementato su Confidential Computing basandosi su apparati HSM FIPS 140-2 Level 3, con ulteriore livello di protezione per i dati in uso.

- **Security Governance on-premise:**

- È necessario implementare un servizio di gestione delle chiavi poiché molte PA non hanno un HSM. La crittografia e la gestione delle chiavi fanno parte dei servizi di sicurezza di base richiesti dal PSN che deve fornire questo servizio.
- Il servizio deve consentire di gestire il ciclo di vita delle chiavi all'interno dei moduli di Key Management definiti all'interno dei *Tenant-Cloud* dei clienti.
- Per quel che riguarda il servizio di Key Management, l'architettura concettuale prevede la costruzione del servizio sfruttando software commerciali forniti da aziende specializzate nel settore, assicurandosi di implementare la corretta affidabilità del servizio stesso, essendo vitale per tutti gli ambienti che saranno definiti. La modalità di fruizione deve essere self-service, e deve essere garantita l'integrazione con i modelli e le interfacce di management previste, in modo da avere coerenza con il modello di gestione previsto dal disegno.
- La soluzione deve consentire le seguenti operazioni:
  - Generazione delle chiavi all'interno di apparati HSM;
  - Backup e restore delle chiavi;
  - Sincronizzazione delle chiavi con i servizi di Key Management del CSP;
  - Monitoraggio e auditing delle operazioni eseguite sulle chiavi;
  - Rotazione delle chiavi manuale e automatica;
  - Revoca della validità delle chiavi.

La crittografia è obbligatoria per tutte le applicazioni e i servizi ospitati nel PSN, mentre i servizi che devono implementare meccanismi di crittografia *at-rest* e/o *in-transit* e che devono integrarsi con il servizio di Key Management, sono quelli presenti nel catalogo servizi del Secure Public Cloud.

2.9.2.2.2 Confidential Computing nell'ambito del PSN

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.

Il Confidential Computing va nella direzione di questi "driver" consentendo ai clienti di incrementare il controllo sul TCB in uso per l'esecuzione dei workload su ambiente Cloud, definendo con precisione tutto l'hardware e il software che ha accesso ai loro workload (dati e codice) e fornendo i meccanismi tecnici per applicare in modo verificabile questa garanzia (enforcement). In breve, è possibile mantenere il pieno controllo sui propri "*secrets*" rimuovendo il CSP dal Trusted Computing Base, riducendo così il confine di protezione solo all'hardware e all'applicazione stessa. Questa modalità consente a molti workload di poter essere utilizzati nel cloud pubblico, con un livello di protezione che si estende fino ad amministratori o utenti direttamente collegandoli all'hardware che esegue applicazioni. È quindi una tecnologia che

aumenta significativamente il grado di fiducia circa la capacità di proteggere la sovranità nel cloud pubblico, e questo lo rende particolarmente rilevante nell'architettura del PSN. Inoltre, grazie alla crescente integrazione delle funzionalità di Confidential Computing nei servizi PaaS, questo maggiore grado di fiducia può essere raggiunto con un impatto ridotto sulla capacità di innovazione fornita dai servizi Public Cloud. Questa combinazione di fattori rende il Confidential Computing una risposta molto efficace alle esigenze di Sovranità e Trasformazione Digitale del PSN.

Quindi i servizi di Confidential Computing consentono la rimozione del Cloud Service Provider dalla *Chain of Trust* a un livello senza precedenti rispetto al passato e offrono il più alto livello di sovranità disponibile oggi sul mercato nel cloud pubblico, migliorando sempre di più sotto questo aspetto. Ciò consente ai clienti e ai governi di soddisfare oggi le proprie esigenze di sovranità e di sfruttare l'innovazione domani.

L'architettura concettuale proposta prevede l'utilizzo del Confidential Computing sia nello scenario di migrazione Lift & Shift che negli scenari di nuove implementazioni o *renew/refactoring* di applicazioni esistenti, che vogliano abbracciare i paradigmi Cloud Native mantenendo un controllo stringente sull'accesso ai dati gestiti e al codice.

Per non compromettere la protezione offerta da questi servizi, occorre che lo stesso livello di controllo sia applicato a tutte le componenti dell'applicazione, in particolare al servizio di Key Management, ai servizi PaaS e/o di containerizzazione eventualmente usati e ai servizi di storage, che devono garantire l'encryption at rest del dato.

In conclusione, il Confidential Computing è una tecnologia all'avanguardia che consente un controllo su dati e risorse senza precedenti, i cui *security enforcement* non vanno a scapito dell'innovazione e della trasformazione digitale abilitate dai servizi cloud. E questa è una risposta solida agli obiettivi del PSN.

2.9.2.2.3 Servizio di Backup

Per la natura di sicurezza intrinseca del PSN, le capacità di governo dei dati della piattaforma sono fondamentali ed è evidente che, per esercitare la sovranità sullo stesso, sia altresì necessario garantire l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP. È per questo motivo che nel servizio Secure Public Cloud è prevista l'implementazione di un ulteriore livello di archiviazione all'interno dei Data Center del PSN per garantire la sovranità del dato. Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup-as-a-service presente nel Private Cloud del PSN in modo che lo Storage su cui risiede il dato protetto sia in completa gestione di personale del PSN. Questa 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 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. Infine, il servizio deve integrarsi con il modello di gestione previsto e consentire il controllo da parte del cliente finale.

2.9.2.3 *Governance*

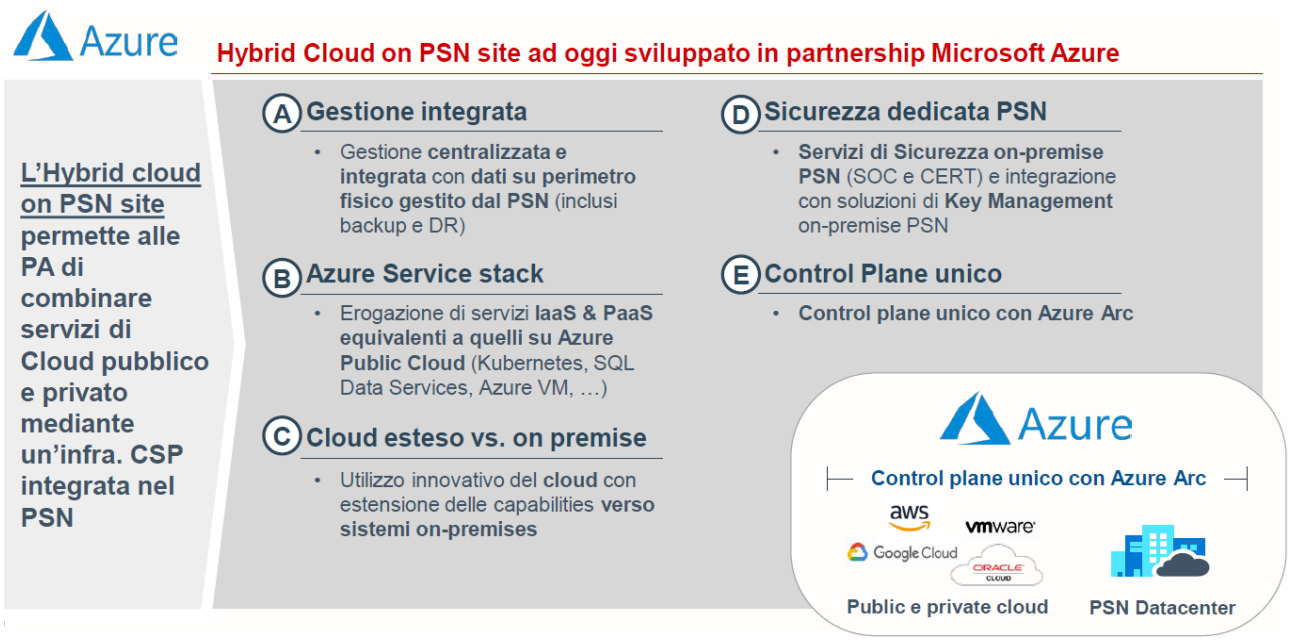
La gestione e la protezione degli account con privilegi amministrativi estesi è di fondamentale importanza per la consistenza del modello. Il disegno prevede che non siano presenti privilegi "persistenti" in nessuno degli ambienti connessi al PSN. Questo criterio si applica sia a tutti i repository di identità di tutti gli attori nonché a tutti i ruoli amministrativi degli ambienti di piattaforma realizzati in entrambi i lati dell'infrastruttura PSN. Il privilegio deve essere assegnato all'attore "candidato" ad assumerlo solo a valle di un processo autorizzativo, per un periodo limitato di tempo. Il processo di attribuzione del ruolo deve essere soggetto ad audit da parte del MSP-PSN e del cliente. Il processo può coinvolgere tutti gli attori sia per la fase autorizzativa (ad esempio cliente che autorizza il MSP ad assumere un ruolo, o responsabile del MSP che autorizza un operatore del MSP ad assumere un ruolo) che per la candidatura al ruolo (ad esempio operatore del MSP candidato al ruolo di contributor, o amministratore del cliente candidato al ruolo di Administrator). Tutti gli utenti che possono assumere ruoli con privilegi amministrativi devono usare meccanismi di autenticazione a più fattori.

Un altro meccanismo importante per l'implementazione del modello è il provisioning degli ambienti con l'applicazione automatica delle Policy, su entrambi i lati dell'infrastruttura del PSN. Questo garantisce che l'autonomia operativa dei clienti non deroghi dalle regole di sicurezza, pur lasciando libertà di implementare le proprie politiche di conduzione IT. Il MSP-PSN è responsabile della gestione del ciclo di vita delle Policy e della loro applicazione ai segmenti.

L'implementazione del servizio prevede la creazione dell'ambiente della PA e la realizzazione di un monitoraggio continuo per la garanzia della sicurezza del perimetro.

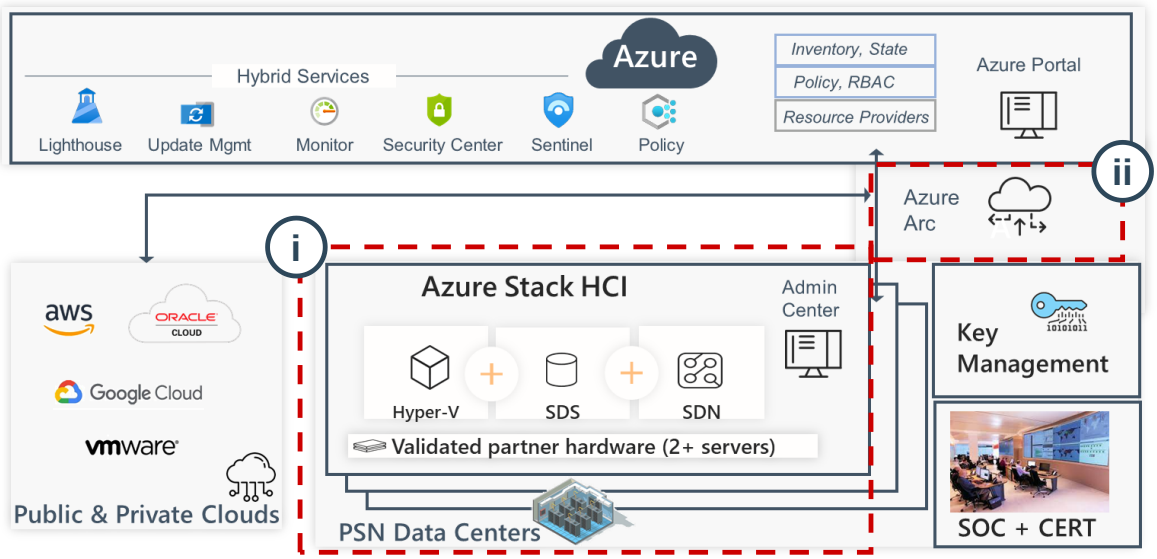
2.9.3 Hybrid Cloud on PSN Site

L'Hybridcloud on PSN site permetterà alle PA di combinare i servizi privati e ibridi dei CSP (Azure), su infrastruttura sicura PSN.



Il servizio mette a disposizione infrastrutture iperconvergenti dedicate:

I. basate su **soluzioni HCI** (Hyperconverged Infrastructure) **dedicate** a ciascun cliente e **ubicate all'interno** dei Data Center del **PSN**;
II. registrate nelle **subscription dei clienti,** che diventeranno «deployment target» utilizzabili attraverso il **control plane di Azure** (Portale, Powershell, CLI, Rest API, ...) per mezzo del servizio Azure Arc.;
III. caratterizzate da un **Management Plane** formato da**:**
   - una componente rimanente sull'**area On-premise** del servizio (Admin Center);
   - una componente che sfrutta i **servizi cloud Azure** per le funzionalità di monitoraggio, gestione aggiornamenti, raccolta eventi di sicurezza e controllo security posture.



Di seguito un focus sui servizi Azure stack HCI e Azure Arc:

I. **Azure stack HCI**
Servizi di network altamente resilienti e consistenti grazie alle funzionalità della Software Defined Network:
   - Infrastrutture implementate sul **paradigma SDDC** con a disposizione **servizi di virtualizzazione delle componenti di Compute, di Storage e di Network** e gestite:
     - **operativamente**, fino all livello Hypervisor, da **personale sistemistico;**
     - dal punto di **vista di sicurezza**, dal **SOC e CERT** del PSN.
   - Specifiche tecniche di un'**infrastruttura dedicata: variazione tra 2 e 16 nodi computazionali** basati su **server certificati** e **validati** per **ottimizzare le performance e la capacity** con:
     - processori di nuova generazione;
     - dimensioni adeguate al consolidamento dei workload;
     - storage Iperconvergente Ibrido (SSD/SAS);
     - infrastruttura di rete ad alte performance (25/40 Gbps).

II. **Azure Arc**

Gestione uniforme ed omogenea dell'infrastruttura *iperconvergente* che garantisce flessibilità in compute e storage:

- **Distribuzione servizi Cloud Native di tipo Paas** *(Orchestrazione di container – Kubernetes; DB-as-a-service - SQL & PostgreSQL; Web App Services - FaaS, Logic App; Machine learning & AI Service; Virtual Desktop-as-a-service).*
- **Gestione da parte dei clienti del ciclo di vita delle virtual machine** su Azure Stack HCI attraverso il portale Azure (come previsto per il servizio Secure Public Cloud o altri servizi su Azure).
- Definizione sulla base di Azure Policy di un **set di policy di sicurezza e di monitoraggio,** che verranno propagate e applicate a tutti i workload integrati tramite Azure Arc in tutti gli ambienti disponibili a partire dal Hybrid Cloud on PSN Site fino ad altri Hyperscaler o ambienti on-premise cliente.

L'architettura concettuale propone una soluzione di tipo "Hybrid Cloud" basata su due componenti principali:

- Un servizio di tipo **Hyperscale Public Cloud** erogato da una *Region* collocata sul territorio nazionale, per la sola erogazione di un **control plane** unificato;

- Un servizio erogato dai Data Center del PSN distribuiti sul territorio Nazionale di tipo "**PSN Private Cloud**" che fornirà le risorse infrastrutturali e le componenti di servizio erogate verso le PA.

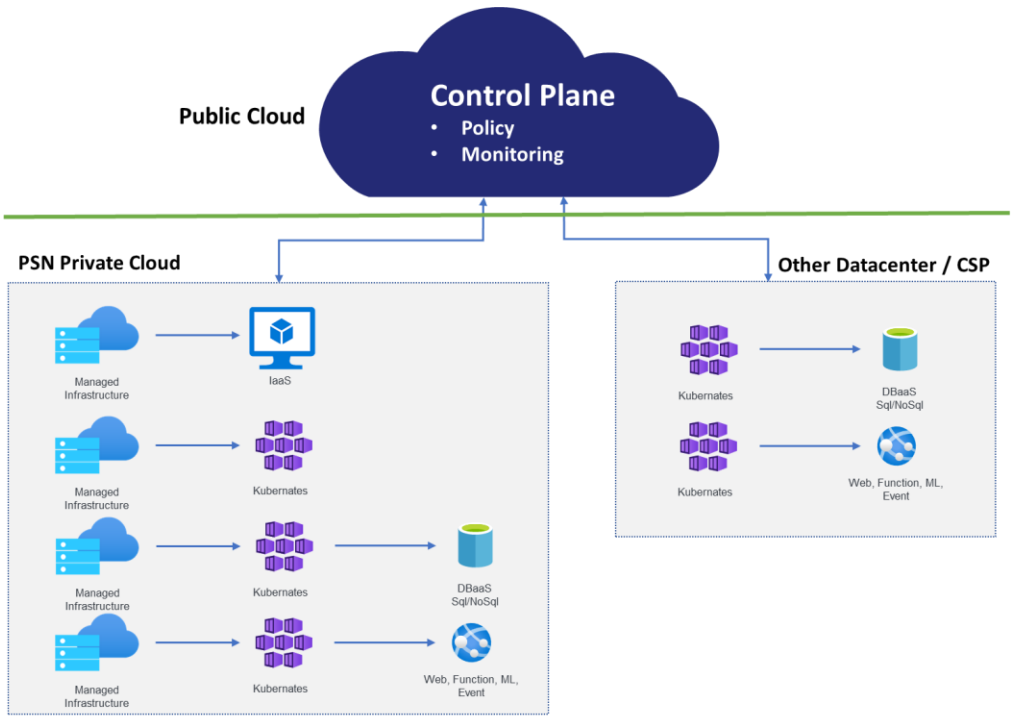


Figura 8: Control Plane e architettura servizio

Il modello di governance prevede l'estensione verso la componente Hosted-On-PSN Private Cloud del modello implementato in ambito Public Cloud grazie a tecnologie che consentono di usare il control plane del Public Cloud anche per governare la componente on-premise o su altri data center.

Il PSN avrà responsabilità di gestione e manutenzione delle componenti hardware e software presenti on-premise che nel modello public cloud sono delegate al CSP.

Ad ogni cliente che aderisce al servizio verrà messa a disposizione una **infrastruttura fisica dedicata** basata su un cluster di server modulare che potrà crescere/decrescere con la granularità del singolo server.

Su questa infrastruttura dedicata (denominata Tenant-On-prem) sarà possibile governare la creazione e gestione di servizi in modalità IaaS e PaaS sfruttando template messi a disposizione ad-hoc, gestiti e aggiornati tramite il control plane unificato su Public Cloud. Inoltre, la gestione della Capacity del cluster fisico dedicato e della relativa variazione delle risorse hardware in uso andrà gestita tramite Service Request che il cliente inserirà su sistema di ITSM dal PSN e che verranno indirizzate tramite opportuni interventi operativi.

La disponibilità di servizi PaaS in ambienti on-premise dovrà essere basata su implementazioni su cluster Kubernetes. In questo scenario, la gestione di questo cluster e delle risorse assegnate ai servizi PaaS rimane in carico al cliente ed avviene in coerenza con il modello di gestione.

L'architettura PSN non prevede livelli di astrazione, come ad esempio portali o strumenti sviluppati ad hoc per la gestione e il controllo degli ambienti, ma, al contrario, fornisce nativamente un'esperienza coerente sia per AppOps (gestito dal cliente stesso) che per DevOps (team operativi applicativi dedicati). Non prevede inoltre una distinzione di gestione e di ambienti tra vecchie e nuove applicazioni o fra adozione di paradigmi IaaS e PaaS. In definitiva, l'architettura consente la predisposizione di ambienti sicuri per tutte le infrastrutture e applicazioni da distribuire sulla piattaforma PSN. Per raggiungere tale obiettivo, qualsiasi sia l'interfaccia utilizzata, il Control Plane e il Management Plane rendono disponibile un modello unico e coerente di gestione di tutte le risorse PSN e dei canali di provisioning/deprovisioning, soggetto a controlli basati sui ruoli (RBAC) e Policy. Quindi tutti gli attori, in base ai loro ruoli e responsabilità, avranno la possibilità di utilizzare lo stesso Control/Management Plane per stabilire un insieme standardizzato di Policy e controlli per governare l'intero patrimonio IT definito nel PSN.

La gestione dell'utente e dei diritti ad esso assegnati permette la segregazione degli stessi in ciascun ambito senza propagazione automatica di diritti tra il mondo Distributed Cloud e quello PSN. Questo sistema flessibile e granulare permette di mantenere le identità ove il ciclo di vita delle stesse garantisce la massima accuratezza, con possibilità di avere set di diritti diversi nei vari contesti e completo controllo dell'attivazione dei privilegi quando necessario. Il sistema di controllo centralizzato permette reportistica accurata e coerente degli accessi e delle assegnazioni dei privilegi nonché delle azioni effettuate sulle risorse target.

L'architettura dell'Hybrid Cloud on PSN on Site deve essere in grado di garantire alti livelli di affidabilità tramite implementazione di soluzioni di astrazione delle risorse fisiche (es. soluzioni

SDDC) che permettano di gestire infrastrutture di elaborazione sottostanti distribuite su diversi data center collegati tra loro a bassa latenza.

L'Hybrid Cloud on PSN on Site fornirà i seguenti servizi:

- IaaS: Creazione e gestione di VM e del logical networking;
- Container as a Services implementato su diverse distribuzioni;
- DBaaS: Servizi di DBaaS basati su software commerciali e open source, quali:
  - PostgreSQL;
  - MySQL;
  - Microsoft SQL DB/SQL Managed Instances;
- PaaS per servizi per l'implementazione di applicazioni ServerLess, quali:
  - Web Application;
  - Function as a Service;
  - Integration services;
  - Eventing as a service;
- NoSQL DBaaS;
- Machine Learning as a service.

Infine, sfruttando le tecnologie di gestione di ambienti Distributed Cloud che proiettano sul control plane del Public Cloud le risorse definite su altri ambienti, siano essi altri Data Center on premise o altri cloud provider, è possibile estendere il modello di gestione anche verso questi altri ambienti, abilitando lo scenario ibrido e multicloud e mantenendo coerenza di automazione, sicurezza, governance e gestione.

2.10 Multi Cloud

A completamento dell'offerta dei servizi Cloud proposti nel presente progetto, la NewCo PSN offre la possibilità di integrarsi con le migliori soluzioni di Public Cloud dei principali player e Cloud Provider internazionali. L'offerta Multicloud si propone come soluzione completa di architetture Hybrid & Multicloud e come interfaccia unica verso il cliente, indipendentemente dal cloud provider di riferimento. Il PSN è in grado di disegnare architetture su misura proponendo al cliente soluzioni basate sulle proprie offerte e sul best-in-class dei Public Cloud Provider, armonizzando e ottimizzando le specifiche logiche per sfruttare al massimo le caratteristiche dei singoli cloud, dei nuovi servizi e delle nuove tecnologie.

2.10.1 Cloud Management Platform

La Console Unica descritta nel documento "*Specificazione delle caratteristiche del servizio*", resa disponibile a tutte le Amministrazioni che contrattualizzeranno servizi proposti nel presente progetto, è applicabile anche in un contesto Multicloud e si integra con le funzionalità della Cloud Management Platform, unico punto di gestione per i servizi standard erogati dal PSN. Attraverso servizi professionali (opzionali) è possibile estendere le capabilities standard con funzionalità aggiuntive o personalizzazione.

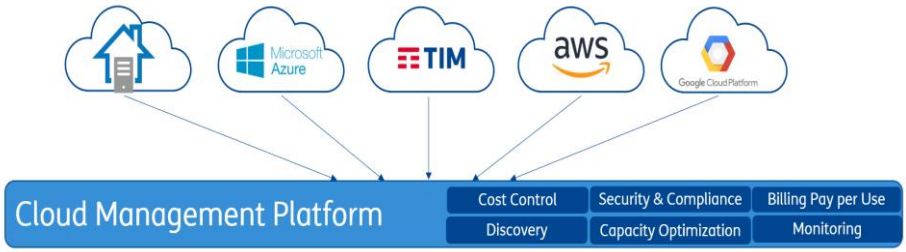


Figura 9: Cloud Management Platform

Pertanto, la Console Unica di Gestione permetterà alle amministrazioni aderenti di gestire i servizi sul PSN e su altri Cloud Service Provider, attraverso le funzionalità riassunte di seguito:

- Portale self-service con catalogo dei servizi unificato;
- Servizi di infrastruttura (designing, provisioning e management di infrastrutture multi-cloud);
- Interazione via API per modelli Cloud Agnostic di IaC (con integrazione Git repositories e strumenti di CI/CD);
- Servizi e BluePrint tecnologiche;
- Dashboard di Performance Monitoring, analisi predittiva e definizione di allarmi per superamento soglie;
- Interfaccia interattiva di misurazione e gestione dei consumi e delle risorse;
- Strumento di costruzione di report di Cost Control e Resource Usage;
- Gestione finanziaria dell'IT.

Sono inoltre disponibili come servizi aggiuntivi (che richiedono in ogni caso attività professionali di configurazione e implementazione su CU e CMP) funzionalità di:

- Governance (diritti di utilizzo, approvazioni, recupero, showback);
- Servizi e BluePrint tecnologiche personalizzati;
- Workflow personalizzati;
- Capacity Planning Avanzato (corretto dimensionamento, modellazione, scenari di tipo "what-if" e funzionalità analitiche basate su modelli di capacità);
- Advanced Monitoring (può richiedere l'installazione di componenti sui server del cliente);
- Security, Compliance & Remediation in ambito MultiCloud (vedi sotto).

2.10.2 Security & Compliance in ambito Multi Cloud

Con la natura dinamica delle applicazioni multi-cloud, è essenziale effettuare frequentemente le operazioni mirate a mantenere la sicurezza e la conformità dei Servizi e delle applicazioni. La piattaforma CMP, opportunamente configurata e personalizzata per le specifiche esigenze delle singole Amministrazioni può automatizzare i test e la correzione della configurazione delle risorse cloud, in modo che i servizi cloud non contengano vulnerabilità dipendenti dalle configurazioni stesse. I controlli di sicurezza effettuati dal software sono basati su policy (ad es.: GDPR, CIS, PCI, Custom) e valutano automaticamente le configurazioni di risorse cloud e container rispetto alle migliori best practices. La funzionalità attivabile di remediation automatica colma rapidamente le lacune e facilita la gestione nel cloud, in AWS, Azure e Google Cloud.

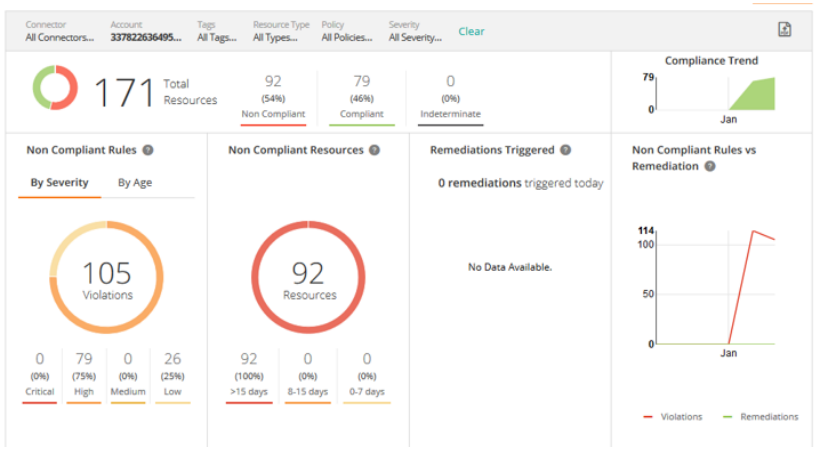


Figura 10: Esempio dashboard Sec&Compliance

2.11 Servizio di Migrazione, Evoluzione e Professional Services

In base al Piano di Digitalizzazione 2020-2022 le PA che utilizzano CED che non soddisfano i parametri definiti nella circolare AgID n. 01 del 14 giugno 2019 non possono fare investimenti di espansione ma dovranno, essere migrati nel Private Cloud della NewCo PSN. A valle della richiesta di poter usufruire dei servizi offerti dalla NewCo PSN, le PA forniranno l'elenco aggiornato del perimetro IT e TLC coinvolto nell'affidamento del servizio, con indicazione delle modalità richieste (Housing, Hosting, IaaS). Tale elenco fornirà gli elementi per poter identificare l'insieme dei Servizi e relative modalità di fruizione e contrattualizzare il rapporto tra la NewCo PSN e le PA.

2.11.1 Figure Professionali

La NewCo PSN renderà disponibili risorse professionali in grado di poter supportare le Amministrazioni in tutte le attività/necessità che si renderanno necessarie nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-host, re-architect, re-platform), proseguendo nella fase di riavvio degli applicativi, regression test e terminando nel supporto all'esercizio.

Per ogni progetto verrà individuata il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste. Il team mix potrà esser composto da una o più delle seguenti figure professionali:

a) **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.

b) **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.

c) **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

d) **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.

e) **Business Analyst**: È responsabile dell'analisi dei dati anche in ottica di business, e della relativa raccolta dei requisiti necessari a migliorare la qualità complessiva dei servizi IT forniti.

f) **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

g) **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

h) **Devops Expert**: Ha consolidata esperienza nelle metodologie di sviluppo DevOps su progetti complessi, per applicare un approccio interfunzionale in grado di garantire la sinergia tra i team di sviluppo e di gestione dei sistemi; è responsabile di progettare le strategie DevOps, identificando gli strumenti di controllo dei sorgenti, di automazione e di rilascio in ottica Continuous Integration e Continuous Development.

i) **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.

j) **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.

k) **UX Designer**: ha una conoscenza teorica e pratica dei principi di usabilità, paradigmi di interazione e principi di interaction design e di gestione delle problematiche di compatibilità cross-browser (desktop, tablet, mobile); è responsabile dell'applicazione dell'approccio centrato sull'utente (human centered) nello sviluppo dei servizi digitali, garantendo il raggiungimento efficace ed efficiente degli obiettivi dell'utente nell'interazione con l'Amministrazione.

l) **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

m) **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.

n) **Security Principal**: Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.

o) **Senior Information Security Consultant**: Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.

p) **Junior Information Security Consultant**: Garantisce l'esecuzione delle misure di sicurezza per proteggere le reti ed i sistemi informatici. Attua le regole definite in materia di sicurezza delle informazioni.

q) **Senior Security Auditor/Analyst**: Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia. Completa i giornali di audit documentando test e risultati dell'audit.

r) **Security Solution Architect**: Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.

s) **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.

t) **Junior Security Analyst**: Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.

u) **Forensic Expert**: E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

v) **Senior Penetration Tester**: Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.

w) **Junior Penetration Tester**: Effettua tentativi di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza in accordo con quanto definito le progetto di riferimento.

x) **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.

y) **Educational Designer/Tutoring:** Struttura, organizza e schedula i programmi di formazione, ne valuta la qualità attraverso un processo di feedback.

2.11.2 Migrazione

I servizi di Migrazione saranno quantificati e valutati economicamente sulla base di specifici assessment da condurre 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, la NewCo PSN metterà a disposizione delle PA le seguenti figure professionali:

1. Un **Project Manager,** che dovrà coordinare le attività e che dovrà collaborare col referente che ogni singola PA dovrà indicare e mettere a disposizione;
2. Un **Technical Team Leader** che seguirà tutte le fasi più strettamente legate agli aspetti operativi.

Si chiederà alla PA la disponibilità di fornire uno o più referenti coi quali il Project Manager e il Technical Team Leader della NewCo 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 NewCo PSN e PA.

A seguito dell'invio del Piano dei Fabbisogni da parte dell'Amministrazione – non descritto nel presente Progetto di fattibilità:

1) verrà indetto, da parte della NewCo PSN, il Kick off di Progetto tra la NewCo PSN e la PA durante il quale verranno identificati gli stakeholders di Progetto della NewCo PSN e della PA.

2) Entro 60 giorni successivi al Kick off di Progetto, la NewCo PSN, avvalendosi del supporto del/dei referenti delle PA, comunicati in sede di Kick off, presenterà il documento "**Progetto del Piano dei Fabbisogni**", contenente il "**Piano di Migrazione di Massima"** dove verranno definite le macro-attività di progetto. La PA, una volta ricevuto il suddetto Progetto del Piano dei Fabbisogni, potrà, entro i successivi 10 giorni, approvarlo, ovvero far pervenire alla NewCo PSN le proprie osservazioni che dovranno essere recepite dalla NewCo PSN entro i successivi 10 giorni lavorativi.

   Ogni Piano di Migrazione sarà articolato secondo i seguenti capitoli descriventi le 4 fasi di Progetto 1) Analisi, 2) Setup, 3) Migrazione, 4) Collaudo.

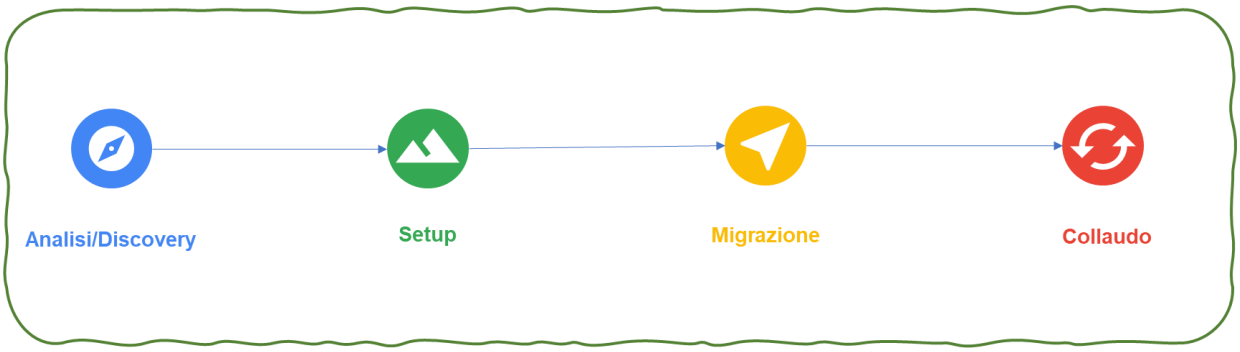


Figura 11: Flusso di Migrazione

I. Analisi/Discovery

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 dell'ambiente da migrare;
i) Energy Optimization.

Al fine di supportare le PA nel processo di adozione del Cloud è necessario identificare un modello per la valutazione oggettiva del livello attuale dell'ente da analizzare e degli interventi di adeguamento necessari. Il modello di riferimento che intendiamo proporre è il Cloud Maturity Model, modello standard che ha lo scopo di definire un approccio strutturato e una serie di controlli

da attuare per valutare il cosiddetto «livello di maturità» attuale del Cloud della PA ed i gap rispetto al livello atteso, al fine di rispettare gli obiettivi del PNRR. L'approccio proposto supporta pienamente e completa le indicazioni di AgID per implementare il processo di evoluzione verso il cloud.

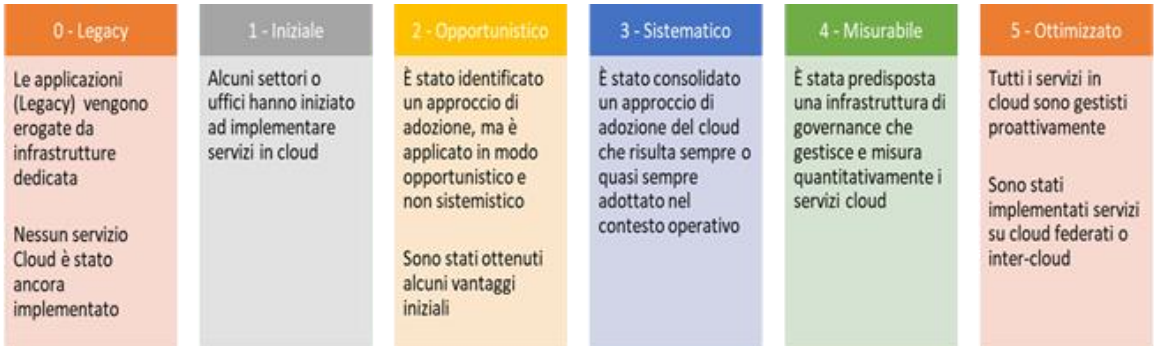


Figura 12: Cloud Maturity Model

Più specificatamente, al fine di valutare correttamente ed efficacemente il livello di maturità si procederà con un assessment. I controlli valuteranno differenti aspetti afferenti a domini tecnici e non tecnici, attraverso la predisposizione di benchmark e di questionari che verranno compilati con il supporto della PA. Al termine di ogni controllo saranno individuati i gap da colmare per portare il livello complessivo di adozione dal valore attuale (current level) fino al valore atteso (target level). La Figura 13 presenta un esempio del livello attuale (in azzurro) e target (in ocra), sui ciascuno dei diversi domini di valutazione individuati.

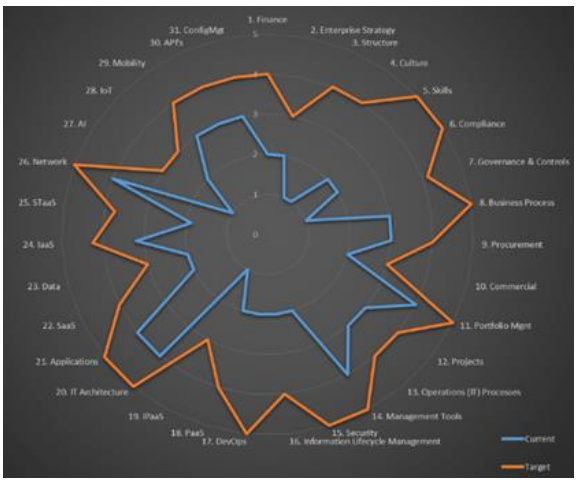


Figura 13: Livelli attuali e target del Cloud Capability Maturity Model

Un approccio basato sulla valutazione del livello di maturità di adozione prevede quindi:

i) l'applicazione del modello per valutare il livello di maturità oggettivo (current) dell'adozione cloud;

ii) la valutazione del gap rispetto al livello atteso;

iii) l'individuazione di interventi focalizzati per migliorare il livello di adozione e raggiungere il livello atteso;

iv) la pianificazione e l'implementazione degli interventi individuati;

v) la verifica ex-post con nuova valutazione del livello di adozione per verificare l'efficacia degli interventi di miglioramento attuati.

Nella fase di Analisi/Discovery sarà anche valutata l'attuale postura in termini di sicurezza applicativa e infrastrutturale attraverso l'uso di analisi DAST e VA effettuati verso le applicazioni esistenti nella PA richiedente.

Inoltre, la **Discovery** ha lo scopo di raccogliere tutte le informazioni relative alla 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, hardware e software migrate. Al termine dell'attività di discovery verrà prodotto un registro della configurazione delle componenti da migrare condiviso e sottoscritto dall'Amministrazione. Le successive fasi della migrazione dovranno stabilire verso quale tipo di infrastruttura, d'accordo con il/i referenti delle PA, sarà indirizzata. Eventuali cambiamenti che si rendessero necessari durante la migrazione, dovranno essere riportati nel registro stesso.

Di seguito si riporta un esempio di possibile registro della configurazione

Componente	Descrizione	Versione/ Modello	Licenza e Manutenzione	Documentazione	Note
S.O. server XYZ	Sistema operativo installato sul server fisico XYZ	Windows Server 2012	Sì, sottoscrizione annuale	Disponibile al link ...	Server per il servizio di cartelle condivise

Al fine di migliorare la sostenibilità energetica della digitalizzazione della PA, verrà erogato un servizio di Energy Optimization atto a valutare ed ottimizzare i consumi energetici dell'infrastruttura e dei workload da migrare. Questo tipo di servizio si basa sull'insieme di tecniche e competenze che vanno sotto il nome di "green computing".

Per quanto riguarda la valutazione, questa verrà fatta assumendo come valore di riferimento il consumo (misurato o stimato sulla base dei valori di targa) dell'infrastruttura prima che questa venga migrata. Seguirà una valutazione circa l'utilizzo delle risorse HW e SW da impegnare nel PSN con il preciso scopo di contenere i consumi, ad esempio valutare la frequenza del processore, la dimensione della memora volatile e di massa, il tipo stesso di processore, etc...

A seguito della migrazione si propone poi una fase di ottimizzazione energetica del workload e dell'hardware, basata su misure di consumo fatte direttamente nelle infrastrutture del PSN.
L'output del processo di ottimizzazione può includere prescrizioni, come ad esempio l'aggiornamento della versione del software al fine di meglio sfruttare le caratteristiche dell'HW, oppure suggerimenti sull'utilizzo degli applicativi.

La scelta della strategia di migrazione sarà effettuata tra quelle indicate nel documento "manuale di abilitazione al cloud" di AgID e note come le 6R (Retain, Retire, Re-purchase, Re-host, Re-platform e Re-architect) e avverrà sulla base delle risultanze dell'analisi dell'ambiente e delle esigenze espresse dalla singola PA. Ad eccezione dei casi di Housing, la migrazione sarà effettuata

principalmente in modalità Re-Host (lift&Shift) che consiste nel "prendere" (Lift) l'intero servizio, compreso di infrastruttura, architettura, dati e traffico e "spostarlo" su un hosting cloud (Shift) senza modifiche al core dell'applicativo. La migrazione potrà esser effettuata in due modalità manuale e automatizzata. Questa strategia permette di effettuare un primo passo verso il cloud lasciando aperta la possibilità, successivamente, di implementare ulteriori miglioramenti all'applicativo che consentano di sfruttare ulteriormente i vantaggi del cloud andando ad utilizzare altre strategie di migrazione previste dal paradigma delle 6R, ossia Re-Platform e Re-Architect.

II. **Setup**
   a) predisposizione dell'infrastruttura target presso i nuovi DC:
      (1) Disegno dei workload;
      (2) Definizione architettura logica e fisica;
      (3) Configurazione ambienti;
   b) se richiesto, come servizio aggiuntivo, predisposizione dell'infrastruttura di networking relativa alla connessione tra la PA e i nuovi DC.

III. **Migrazione**
   a) Trasferimento dei dati;
   b) Implementazione policy di sicurezza;
   c) Impostazione del monitoraggio.

IV. **Collaudo**
   a) Finalizzato a testare le procedure e modalità della migrazione. A seguito del collaudo funzionale della intera infrastruttura di ogni PA, la NewCo PSN dovrà prevedere l'attivazione di tutti i Servizi richiesti dalla PA (riferimento §. 2.3.5 Collaudi e verifiche di conformità del documento "*Specificazione delle caratteristiche del servizio e della gestione*").

Tutte le fasi di migrazione verranno eseguite tenendo conto di:

a) Valutazione dei Rischi;
b) Conduzione di Misure Specifiche di Valutazione del Rischio e Esecuzione di Test Preliminari;
c) Definizione delle Strategie di Mitigazione e delle Contromisure;
d) Definizione dei metodi di Monitoraggio del Rischio e dei Punti di Controllo (checkpoint) durante la Trasformazione;
e) Monitoraggio continuo del Rischio durante tutte le fasi di progetto.

3) Entro **60 giorni** dall'approvazione da parte della PA del Progetto del Piano di Fabbisogni, contenente il Piano di Migrazione di Massima, la NewCo PSN, avvalendosi del supporto del/dei referenti delle PA, comunicati in sede di Kick off, definirà e consegnerà alla PA il "**Piano di Migrazione di Dettaglio"** contenente le tempistiche e il dettaglio delle modalità operative di quanto contenuto nel Piano di Migrazione di Massima.
   Nello specifico, Il "Piano di Migrazione di Dettaglio" dovrà evidenziare gli aspetti logistici, infrastrutturale, organizzativi e procedurali previsti per l'erogazione di quanto contenuto nel

Piano di Migrazione di Massima, nonché la pianificazione temporale con cui verranno effettuate le attività.
La PA, una volta ricevuto il suddetto "**Piano di Migrazione di Dettaglio"**, potrà, entro i successivi 10 giorni approvarlo, ovvero far pervenire alla NewCo PSN le proprie osservazioni che dovranno essere recepite dalla NewCo PSN entro i successivi 10 giorni lavorativi.

2.11.3 Servizi di Evoluzione

La NewCo PSN renderà disponibili alle Amministrazioni 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 forniti, afferenti alle 6R delle strategie di migrazione al cloud, saranno 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, verrà proposto un **team mix** composto dai profili professionali sopra elencati.

2.11.3.1 *Re-platform*

La strategia di Re-platform oltre a trasferire un applicativo sul cloud come avviene nel re-host, sostituisce nel processo di migrazione alcune componenti per meglio sfruttare le specificità della piattaforma di destinazione. La finalità principale della strategia è di trasferire l'applicativo in cloud senza stravolgimenti funzionali, analizzando i possibili interventi che consentono di cogliere, rispetto ai benefici garantiti da una soluzione cloud-native, il livello massimo di ottimizzazione e beneficio. Gli interventi si concentrano sul cambio di SO/DB, Software Update, DB Update con l'obiettivo di standardizzare le componenti infrastrutturali e permetterne una più semplice gestione di configurazione. Il servizio può rendersi necessario qualora il livello di sicurezza non sia conforme allo standard minimo; pertanto realizza la modifica di componenti specifici di un'applicazione verso sistemi IaaS e PaaS erogati dal PSN al fine di migliorarne la scalabilità ma soprattutto la sicurezza.

Di seguito vengono illustrati i diversi step del processo di Re-platform:

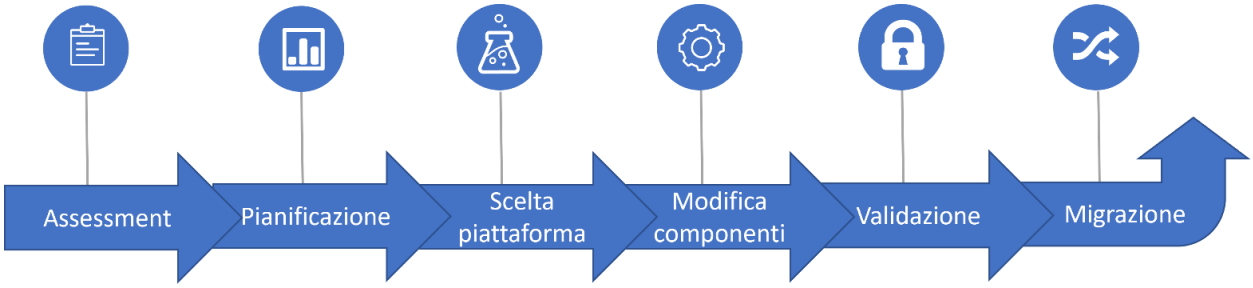


Figura 14: Flusso processo di Re-platform

Nella fase di *Assessment* viene condotta un'analisi dell'applicazione per comprenderne le caratteristiche e poter valutare se la strategia di Re-platform sia adatta allo scopo, definendo le componenti dell'applicazione che possono essere sostituite.

In particolare, alcune delle caratteristiche che vengono analizzate sono:

- architetture modulari e a componenti separabili a diversi livelli di granularità;
- uso di componenti sostituibili con l'equivalente servizio cloud-native;
- eventuali dipendenze dall'hardware fisico;
- disponibilità e modificabilità del codice sorgente;
- criticità legate a componenti sostituibili con un'alternativa cloud native;
- disponibilità di documentazione tecnica che supporti nella sostituzione delle componenti.

Dopo l'Assessment dell'applicativo, segue una fase di *Pianificazione* della migrazione ed una successiva *Scelta della piattaforma* cloud tra quelle disponibili nel catalogo. Successivamente vengono *Modificati i componenti* con quelli individuati in fase di assessment, viene validata la soluzione e infine l'applicazione viene *Migrata* sulla piattaforma PSN.

I vantaggi offerti da un servizio di Re-platform sono:

- ottimizzazione delle risorse e dei costi in quanto permette di utilizzare le caratteristiche dell'infrastruttura cloud senza richiedere modifiche significative agli applicativi;
- tempi di migrazione più rapidi rispetto a un refactoring completo;
- ottimizzazione delle caratteristiche del cloud in termini di disponibilità, scalabilità, osservabilità, resilienza, provisioning delle risorse e sicurezza rispetto ad un approccio lift&shift

2.11.3.2 *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.

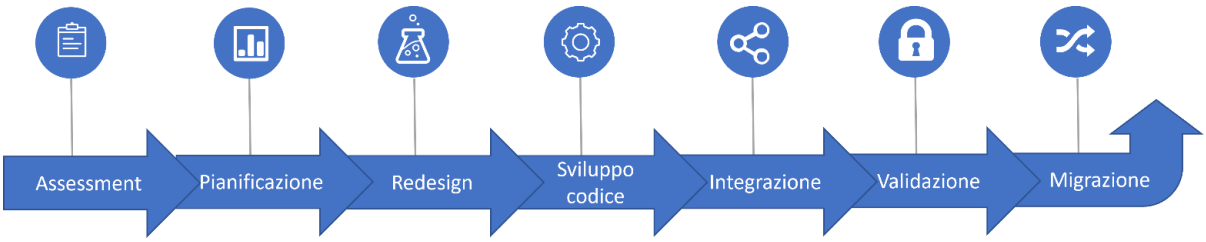


Figura 15: Flusso processo di Re-architect

Nella fase di *Assessment* viene analizzata l'applicazione per comprenderne le caratteristiche in modo da valutarne se la strategia di Re-architect sia adatta per quella specifica applicazione.
In particolare, alcune delle caratteristiche che vengono analizzate sono:

- frequenza di modifiche del codice;
- variabilità dei carichi di lavoro dovuto a picchi di traffico;
- criticità dal punto di vista business;
- architettura completa e Stack tecnologico utilizzato;
- uso di componenti sostituibili con l'equivalente servizio cloud-native;
- disponibilità e modificabilità del codice sorgente;
- criticità legate a componenti sostituibili con un'alternativa cloud native;

- disponibilità di documentazione tecnica completa del codice sorgente.

Dopo l'*Assessment* dell'applicativo, segue una fase di *Pianificazione* di migrazione, seguita da un *Redesign* minimale dell'applicazione per permettere una efficace migrazione. Le fasi successive comprendono interventi sul codice sorgente (*Sviluppo*) nei punti più critici che ostacolano il porting nel PSN, la verifica delle *Integrazioni* necessarie, la *Validazione* della nuova soluzione e, infine, la migrazione dell'applicazione sulla piattaforma PSN.

I vantaggi offerti da un servizio di Re-architect sono i seguenti:

- ottimizzazione dei costi e delle risorse nel lungo termine grazie all'utilizzo delle risorse basato sull'effettiva necessità;
- migliore sfruttamento delle caratteristiche del cloud come disponibilità, scalabilità, osservabilità, resilienza, provisioning delle risorse e sicurezza;
- responsività alle variazioni di carico impreviste grazie ad uno scaling in real time, possibile sulla nuova soluzione;
- incremento della sicurezza grazie anche alla disponibilità di funzionalità avanzate, fornite nella nuova piattaforma PSN.

2.11.4 Professional Services

La NewCo PSN renderà disponibili i servizi professionali sia nell'ottica del mantenimento ed accompagnamento della PA in un percorso evolutivo di IT Digital Transformation, sia in quello di proposizioni maggiormente innovative compresi i servizi legati al rifacimento/sviluppo applicativo.

La NewCo PSN prevede l'erogazione di servizi di Demand Management finalizzati alla raccolta e alla strutturazione delle esigenze di evoluzione e sviluppo dei processi, dei servizi e dei progetti delle Amministrazioni aderenti al PSN. Le attività di Demand Management prevedono l'identificazione e la comprensione dei requisiti di business delle strutture organizzative dell'Amministrazione, al fine di renderli coerenti rispetto alla strategia di evoluzione generale dell'Amministrazione. L'analisi dei requisiti abilita inoltre la definizione delle priorità, rispetto a criteri di scelta concordati con l'Amministrazione, in ottica di efficientamento e generazione di valore aggiunto.

In particolare, il servizio prevede l'esecuzione delle seguenti principali attività:

- Supporto nell'interazione di alto livello con le strutture organizzative per la definizione delle strategie, degli obiettivi e delle direttrici di evoluzioni dei processi, dei servizi e delle applicazioni;
- Conduzione di processi strutturati di raccolta e stesura, in forma strutturata e standardizzata, dei macro-requisiti progettuali;
- Identificazione e valutazione dei requisiti di business e delle esigenze espresse dalle strutture organizzative dell'Amministrazione;

- Valutazione, di concerto con l'Amministrazione, dell'aderenza di quanto realizzato rispetto ai requisiti raccolti e di coerenza rispetto a tempi e costi di implementazione delle soluzioni

In seguito all'avvenuta migrazione, la NewCo PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni. Pertanto, l'Amministrazione potrà decidere di affidare alla NewCo PSN la gestione dell'ambiente tenendo per sé solamente la componente relativa al codice applicativo. Per il corretto svolgimento delle attività verrà reso disponibile, per ogni PA, 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 la NewCo 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 sopra elencati, in base all'ambiente dell'Amministrazione ed ai requisiti della stessa.

2.11.5 Scenari di Migrazione

La strategia di migrazione si basa su un concetto di tailoring per definire il miglior processo di migrazione da proporre all'Amministrazione.

I driver per il tailoring sono:

1. Dimensione dell'amministrazione. Si ipotizza la seguente classificazione:
- ✓ PA di piccole dimensioni: fino a 10 Rack;
- ✓ PA di medie dimensioni: fino a 20 Rack;
- ✓ PA di grandi dimensioni: oltre 20 Rack.

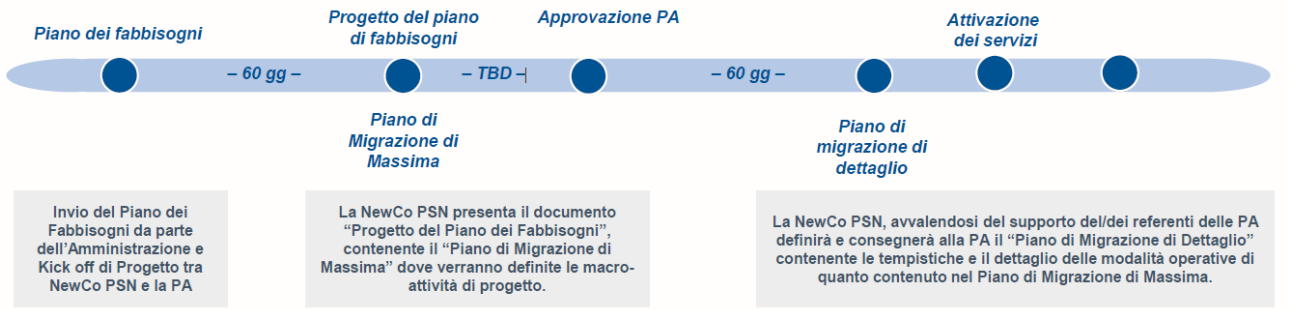
2. Livello di maturità dell'Amministrazione, in base alle risultanze del Cloud Maturity Model.

0 - Legacy	1 - Iniziale	2 - Opportunistico	3 - Sistematico	4 - Misurabile	5 - Ottimizzato
Le applicazioni (Legacy) vengono erogate da infrastrutture dedicata Nessun servizio Cloud è stato ancora implementato	Alcuni settori o uffici hanno iniziato ad implementare servizi in cloud	È stato identificato un approccio di adozione, ma è applicato in modo opportunistico e non sistemistico Sono stati ottenuti alcuni vantaggi iniziali	È stato consolidato un approccio di adozione del cloud che risulta sempre o quasi sempre adottato nel contesto operativo	È stata predisposta una infrastruttura di governance che gestisce e misura quantitativamente i servizi cloud	Tutti i servizi in cloud sono gestisti proattivamente Sono stati implementati servizi su cloud federati o inter-cloud

In base ai driver, il tailoring può dare luogo a 3 differenti scenari di complessità: bassa, media, alta.

Per quanto attiene alle tempistiche previste per il piano di migrazione, in figura una proposta a titolo esemplificativo che può essere declinata in funzione di diversi scenari:

		Dimensione PA		
		Piccola	Media	Grande
Cloud Maturity	0 - Legacy	media	alta	alta
	1 - Iniziale	media	media	alta
	2 - Opportunistico	bassa	media	alta
	3 - Sistemistico	bassa	media	media
	4 - Misurabile	bassa	bassa	media
	5 - Ottimizzato	bassa	bassa	bassa



Scenario 1 alta complessità. Il "Piano di Migrazione di Dettaglio" dovrà evidenziare gli aspetti logistici, infrastrutturali, organizzativi e procedurali previsti per l'erogazione di quanto contenuto nel Piano di Migrazione di Massima, nonché la pianificazione temporale con cui verranno effettuate le attività.

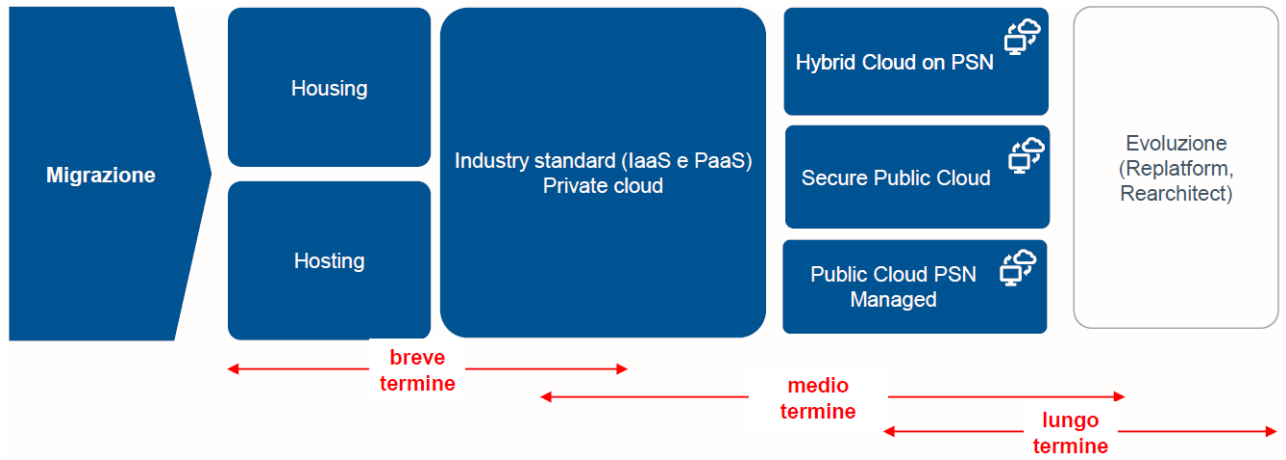
Scenario 2 media complessità. Il Piano conterrà anche la proposta di migrazione/evoluzione a medio termine.

Scenario 3 bassa complessità. Il Piano conterrà anche le proposte di migrazione/evoluzione a medio e lungo termine.

In base al livello di maturità dell'Amministrazione e alle necessità di classificazione dati, si proporrà un diverso Piano di Migrazione.

Breve termine
Ad eccezione dei casi di Housing, la migrazione sarà effettuata principalmente in modalità Re-Host (lift&Shift) che consiste nel "prendere" (Lift) l'intero servizio, compreso di infrastruttura, architettura, dati e traffico e "spostarlo" (Shift) su un hosting cloud senza modifiche al core dell'applicativo.

Medio e lungo termine
Questa strategia permette di effettuare un primo passo verso il cloud lasciando aperta la possibilità, successivamente, di implementare ulteriori miglioramenti all'applicativo che consentano di sfruttare ulteriormente i vantaggi del cloud andando ad utilizzare altre strategie di migrazione nel **medio e lungo termine** previste dal paradigma delle 6R, ossia Re-Platform e Re-Architect.



La NewCo PSN renderà disponibili alle Amministrazioni 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;

		Piano di Migrazione		
		Breve termine	**Medio termine**	**Lungo Termine**
Cloud Maturity	**0 - Legacy**	Housing / Hosting	Hosting / Industry standard Private cloud	Evoluzione (Replatform, Rearchitect)
	1 - Iniziale	Hosting	Hosting / Industry standard Private cloud	Evoluzione (Replatform, Rearchitect)
	2 - Opportunistico	Hosting / Industry standard Private cloud	Industry Standard Private Cloud	Evoluzione (Replatform, Rearchitect)
	3 - Sistemistico	Hosting / Industry standard Private cloud	Industry Standard Private Cloud	Evoluzione (Replatform, Rearchitect)
	4 - Misurabile	Hosting / Industry standard Private cloud	Evoluzione (Replatform, Rearchitect)	Evoluzione (Replatform, Rearchitect)
	5 - Ottimizzato	Hosting / Industry standard Private cloud	Evoluzione (Replatform, Rearchitect)	Evoluzione (Replatform, Rearchitect)
		Hybrid Cloud on PSN		
		Secure Public Cloud		
		Public Cloud PSN Managed		

- ✓ **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.

2.11.6 Servizio opzionale di moving fisico

Il servizio di Housing descritto al § 2.1 del presente documento, prevede che la consegna degli apparati da ospitare presso il Data Center della Newco sia in carico al cliente.
Come elemento aggiuntivo opzionale, la NewCo PSN offre la possibilità alle PA che ne faranno richiesta, di fruire di un servizio di trasloco (Asset Moving), spostamento di asset in gestione, verso il sito PSN presso il quale sarà stato contrattualizzato l'Housing degli asset. Le macro-attività comprese nel servizio includono:

- verifica del back-up della macchina, lo smontaggio dell'apparato nella sede di partenza, lo spostamento inclusi i costi di assicurazione e di trasporto, il rimontaggio dell'apparato nella sede di destinazione, il cablaggio per la connessione alla rete, il collaudo della funzionalità dell'apparato, più ogni altra attività necessaria all'abilitazione della piena operatività del sistema;
- eventuali sopralluoghi nelle sedi di partenza e di destinazione necessari alla presa in carico dell'attività, all'identificazione delle eventuali criticità e alla definizione di accordi operativi con i Referenti dell'amministrazione contraente.

Il servizio è sottoposto ad alcuni vincoli, in particolare:

- il cliente deve garantire la possibilità di movimentazione in sicurezza degli apparati dalla sala server al piano stradale;
- il servizio non si fa carico di eventuali condizioni sulla manutenzione posta dai vendor in caso di movimentazione dell'asset.

2.12 Business & Culture Enablement

La trasformazione digitale deve essere accompagnata non solo da una innovazione tecnologica, ma soprattutto da un cambiamento delle metodologie di lavoro e dall'organizzazione dello stesso. Cambiare la cultura delle Amministrazioni vuol dire agire sulla leadership e sulla collaborazione tra le persone.

Disegnare e produrre servizi e prodotti per i cittadini e per l'imprese completamente digitali, vuol dire anche lavorare allo stesso modo; l'attenzione alle persone ed ai servizi loro erogati consente infatti di rendere questa cultura normale all'interno dell'Amministrazione e quindi poterla replicare più facilmente per i cittadini e le imprese.

Punti nodali di questa trasformazione sono il change management ed il modello formativo. Per questi motivi, la NewCo PSN prevede di mettere a disposizione delle amministrazioni entrambi questi servizi.

Per quanto riguarda il Change Management si prevede un servizio di consulenza organizzativa che progetterà con le Amministrazioni i passi per eseguire il processo di digital trasformation relativamente a:

- Modello organizzativo.

- Competenze e modello manageriale.
- Tool Collaborativi.
- Employee experience.
- Modello di innovazione.

Inoltre. un servizio che consente di erogare formazione tramite l'uso delle tecnologie multimediali e offrire la possibilità di erogare digitalmente i contenuti attraverso Internet o reti Intranet. Per l'utente rappresenta una soluzione di apprendimento flessibile, in quanto personalizzabile e facilmente accessibile.

Il servizio prevede l'erogazione, su una piattaforma messa a disposizione dal PSN, di **corsi base** a catalogo differenziati in base alle esigenze formative e **corsi personalizzati** secondo le esigenze dell'Amministrazione. In aggiunta ai due servizi precedentemente indicati se ne definisce uno di **supporto specialistico** per gli ulteriori aspetti metodologici e didattici, che prevede:

- affiancamento all'utente volto ad istruirlo all'uso delle funzioni del sistema di e-learning;
- gestione della comunicazione con gli utenti tramite i sistemi di messaggistica della piattaforma;
- formazione trasversale con corsi specifici definiti a catalogo e/o customizzati su esigenze dell'Amministrazione su:
    - servizi Cloud ed elementi di innovazione ed ottimizzazione
    - migrazione e analisi degli adeguamenti normativi e degli standard come quelli descritti, ad esempio, nei programmi di Digital Transformation indicati da AgID;
    - formazione verticale su metodologie e processi Cloud, necessarie per governare gli ambienti ed i servizi;
    - formazione su tecnologie Cloud illustrando i vantaggi/benefici di tale servizio;
    - formazione specifica a supporto degli ambienti implementati e dell'offerta degli strumenti del PSN

Inoltre, il PSN renderà disponibile la piattaforma ed il supporto specialistico per i seguenti ambiti:

- amministrativo/organizzativo
- tecnologico

L'area amministrativo/organizzativo prevede i seguenti servizi base:

- validazione e controllo dei risultati delle elaborazioni;
- aggiornamento e manutenzione del data base;
- reportistica e monitoraggio.

L'area tecnologica prevede i seguenti servizi base:

- processi di creazione, classificazione e archiviazione dei contenuti della piattaforma;
- gestione del repository dei contenuti della piattaforma: gestione del ciclo di vita e delle versioni dei contenuti, gestione degli accessi, supporto per contenuti multimediali;
- caricamento di nuovi corsi di auto addestramento e/o aggiornamento di corsi esistenti;
- attività di gestione delle utenze interne/esterne al sistema di e-learning.

Per i corsi ad hoc è previsto un servizio di predisposizione del materiale didattico (realizzazione di WBT) che adotterà standard di mercato per la produzione (learning object, SCORM, ecc...) e logiche di interattività e di costo differenziate, così come indicato nel documento AgID per la realizzazione dei contenuti didattici. Tra questi si distinguono:

- corsi base di tipo generale: usualmente si trovano nei cataloghi dei vari fornitori e fanno riferimento a temi di utilità comune; si prevede di erogare corsi a catalogo con pacchetti da 8 WBT ognuno.
- corsi ad hoc a bassa, media e alta interazione in accordo con le metriche indicate da AgID.

In base alle necessità delle singole amministrazioni verrà individuato il mix di figure professionali necessarie, tra quelle messe a disposizione dalla NewCo PSN, che effettuerà le attività richieste.

3 Sicurezza

La NewCo PSN si doterà di idonee unità organizzative al fine di garantire e assicurare la tutela delle infrastrutture e dei servizi considerati essenziali agli interessi nazionali e alla sicurezza nazionale; in particolare, istituirà al suo interno una Organizzazione di Sicurezza, con elementi caratteristici di autonomia e indipendenza. Tale unità sarà anche preposta alle attività aziendali rilevanti per la sicurezza nazionale e ne sarà garantito il coinvolgimento nelle attività di governance, in particolare riguardo ai processi decisionali afferenti ad attività strategiche e di interesse nazionale.

Il responsabile di tale organizzazione potrà essere individuato in accordo con le autorità istituzionali competenti e dotato di specifici requisiti (es. NOS, cittadinanza italiana).

L'Organizzazione di Sicurezza garantirà la conformità e avrà l'obiettivo di:

- garantire una protezione dell'informazione adeguata in termini di confidenzialità, integrità e disponibilità;
- proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- assicurare la conformità alle leggi e ai regolamenti applicabili, tra cui quelle inerenti la sicurezza delle informazioni, la tutela dei dati personali nonché quelle applicabili agli Operatori dei Servizi Essenziali (OSE), ai Fornitori di Servizi Digitali (FSD) ed ai soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC);
- assicurare un modello strutturale alla protezione dell'informazione e alla gestione dei rischi correlati;
- rispondere in modo efficace alle crescenti minacce ai sistemi informativi nello spazio cibernetico.

Le misure tecniche ed organizzative dovranno essere identificate ed implementate ai sensi delle normative vigenti; saranno inoltre soggette a certificazione ISO/IEC 27001 e ISO 22301 e saranno descritte da specifiche Security Policy elaborate a cura dell'Organizzazione di Sicurezza, in particolare con riferimento alla sicurezza e alla conformità dei sistemi informatici e delle infrastrutture delle reti.

Nel dettaglio, tali Security Policy, che rappresentano gli obiettivi ed i principi di base che devono essere rispettati nella conduzione dei servizi oggetto della fornitura, saranno definite in conformità alle normative applicabili e elencate al § 3.1. Le regole, le procedure operative ed organizzative attuative delle suddette Policy saranno invece riportate nelle procedure di cui al § 3.3.

Il Centro Servizi si impegna inoltre a offrire un continuo miglioramento dei processi attuati in aderenza alle Security Policy di cui sopra e un utilizzo ottimale delle risorse impiegate.

L'Organizzazione di Sicurezza predisporrà uno specifico e dettagliato Piano di Sicurezza redatto in conformità con i criteri di accreditamento AgID relativi ai PSN, che conterrà i) una sintesi delle normative di riferimento applicabili; ii) una generale ricognizione degli asset informatici; iii) le criticità anche potenziali, gli obiettivi di sviluppo, manutenzione e gestione atti a garantire la

corretta erogazione dei servizi; *iv)* le risorse strumentali ed economiche necessarie. In aggiunta saranno integrati elementi relativi alle modalità logistiche ed organizzative, agli strumenti ed ai sistemi che la NewCo PSN adotterà o di cui è provvisto per rendere sicuro e protetto l'ambiente in cui sono ospitati le infrastrutture (Data Center).

Tale Piano sarà revisionato e aggiornato con cadenza almeno annuale e, comunque, ogniqualvolta si dovessero presentare evenienze tali da generare modifiche delle esigenze di sicurezza nella erogazione dei servizi oggetto di fornitura ascrivibili a *i)* ragioni organizzative, procedurali, tecnologiche; *ii)* ad eventuali input della revisione ciclica del sistema di gestione; *iii)* a indicazioni provenienti dai processi di gestione della sicurezza e dall'analisi dei rischi di sicurezza. Tale attività di aggiornamento si svilupperà anche al fine di indirizzare il miglioramento continuo del livello di efficienza dei processi di sicurezza e alla Mission del Centro Servizi.

All'Organizzazione di Sicurezza saranno inoltre attribuiti compiti di controllo e supervisione in relazione alla corretta implementazione nei vari ambiti operativi del Centro Servizi, secondo quanto indicato dalle Security Policy; esse saranno opportunamente definite secondo procedure periodicamente aggiornate. Il personale deputato ad effettuare tali attività di verifica potrebbe essere abilitato secondo criteri definiti dagli organi istituzionali competenti (es. dotati di NOS) e avrà il compito di effettuare, secondo modalità e termini definiti, le verifiche per l'accertamento della sussistenza dei requisiti di sicurezza.

In particolare, saranno eseguite attività di analisi del rischio di sicurezza:

a. nell'ambito dei progetti, per la identificazione dei requisiti di protezione e controllo;

b. sui servizi di erogazione per verificare l'adeguatezza dei controlli in essere, identificare eventuali scostamenti ed identificare le azioni di rientro.

L'analisi dei rischi dovrà essere ripetibile e condotta mediante appositi strumenti di valutazione che permettano anche il tracciamento delle azioni di rimedio eventualmente identificate.

Per ciascuno dei tre modelli di cloud saranno garantiti livelli equivalenti di sicurezza; per il Secure Public Cloud saranno utilizzati i controlli di sicurezza disponibili dal Public Cloud Provider, con l'aggiunta, se necessario, di quelli ulteriori individuati dall'analisi del rischio e dalle necessità di conformità normativa.

Sul piano delle operations, l'Organizzazione di Sicurezza, svilupperà, in particolare, le funzioni di Security Operation Center (SOC) e di Computer Emergency Response Team (CERT) e garantirà tutti i livelli di sicurezza previsti dalle normative vigenti (cfr. par 3.1), la presenza di un ambiente sicuro e protetto e la protezione dei dati personali trattati.
In generale saranno svolte le seguenti attività a contenuto operativo:

- End Point Security;
- Identity & Access Management;
- Key Management;

- Security Platform Management;
- Security Policy Management & Enforcement;
- Real Time Security Monitoring;
- Security Testing & Vulnerability Management;
- Threat Intelligence&Infosharing;
- Incident Response;
- Training & Awareness;

In generale l'Organizzazione di Sicurezza, si farà carico di tutte le attività di progettazione e set up della Gestione della Sicurezza IT, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

3.1 Normative e standard di riferimento

Tenendo in considerazione le esigenze di sicurezza di una infrastruttura dedicata a fornire servizi Cloud e l'evoluzione costante del contesto tecnologico/normativo fortemente enfatizzata dalla recente pubblicazione di direttive, regolamenti, norme e decreti a livello UE e nazionale, il Centro Servizi messo a disposizione dalla NewCo PSN dovrà implementare i più avanzati standard di sicurezza delle informazioni e garantire la conformità, propria e dei propri clienti, ai requisiti cogenti.

Le principali esigenze di sicurezza riguardano:

- la presenza di un ambiente sicuro e protetto;
- la protezione dei dati personali trattati;
- la conformità normativa e di settore del Centro Servizi e dei clienti;

L'erogazione dei servizi ed i sistemi coinvolti soddisferanno pienamente, quindi, i seguenti dispositivi di legge:

- **D.Lgs. 7 marzo 2005, n. 82 e s.m.i** ("Codice dell'Amministrazione Digitale");
- **Piano Triennale per l'Informatica 2020 – 2022** ("Piano triennale per l'informatica nella Pubblica Amministrazione");
- **DPCM del 17/02/2017** («Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali»);
- **D. Lgs. 65/2018 e s.m.i.**, che attua la direttiva UE 2016/1148 (Direttiva «NIS»), intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, applicati agli «Operatori di Servizi Essenziali» (OSE) e ai «Fornitori di Servizi Digitali «(FSD);
- **D.L. 105/2019** (convertito con modificazioni dalla L. 18 novembre 2019, n. 133), come adeguato a sua volta dalla legge n. 8 del 28 febbraio 2020 e dal D.L. 82/2021, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, e i DPCM (tra

cui il 131/2020, entrato in vigore il 5/11/2020) e regolamenti di successiva emanazione (alla data DPR 54/2021 e DPCM 81/2021), come previsti dalla menzionata legge;

- **DPCM n. 131 del 30 luglio 2020** "Regolamento in materia di Perimetro di Sicurezza Nazionale Cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";
- **DPCM n. 81 del 14 aprile 2021** "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;
- **DPR n. 54 del 5 febbraio 2021** "Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
- **DPCM 15 giugno 2021** "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;"
- **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*Regolamento Generale sulla Protezione dei Dati o GDPR*);
- **D.Lgs. 196/2003**, modificato dal D.Lgs. 10 agosto 2018, n. 101 ("Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE");
- **D.L. 65/2018, "**Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
- **D.L. 82/2021 (convertito con modificazioni dalla L. 4 agosto 2021, n. 109)** "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale";

Saranno inoltre considerati come standard di realizzazione e gestione le seguenti linee guida e framework nazionali/internazionali:

- **Piano nazionale per la protezione cibernetica e la sicurezza informatica;**
- **Framework nazionale di cyber security e data protection;**
- **NIST Cyber Security Framework;**
- CIRCOLARE N. 2 del 9 aprile 2018 **Criteri per la qualificazione dei Cloud Service Provider per la PA;**

- CIRCOLARE N. 01 del 14 giugno 2019 **Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;**
- **Misure minime** di sicurezza informatica per la PA (AgID GG.UU 4/2017);
- **ISO/IEC 27000** (Adozione, Implementazione e gestione di un Sistema di Gestione per la Sicurezza delle Informazioni, ed in particolare:
    - **ISO/IEC 27001** – Information technology — Security techniques — Information security management systems — Requirements;
    - **ISO/IEC 27002** - Information technology — Security techniques — Code of practice for information security controls;
    - **ISO/IEC 27701** – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines;
    - **ISO/IEC 27017** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
    - **ISO/IEC 27018 -** Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
    - **ISO/IEC 27005** - Information technology — Security techniques — Information security risk management;
- **ISO 31000:2018** - Gestione del rischio - Linee guida;
- **Cloud Security Alliance** Controls;

Tutti i membri della NewCo PSN sono in possesso della certificazione, in corso di validità, del Sistema di Gestione per la Sicurezza delle informazioni relativamente a tutti i Centri Servizi presso i quali sarà prestato il Servizio – rilasciata in conformità alla ISO/IEC 27001 da un ente di certificazione accreditato da ACCREDIA o da altro ente di Accreditamento firmatario degli accordi di Mutuo riconoscimento.

3.2 Personale e Competenze

Il personale che sarà utilizzato dalla NewCo PSN per la governance e la gestione della sicurezza avrà elevate conoscenze e competenze in materia di Cyber Security, in base al profilo utilizzato, nonché esperienza lavorativa nel settore.

Le risorse impiegate nell'ambito del progetto saranno di alto profilo, sotto l'aspetto dell'esperienza, delle conoscenze e delle competenze. In particolare, saranno impiegati profili di tipo Master, Senior o Expert, laddove richiesto, con competenze multidisciplinari di sicurezza.

Le risorse avranno ampia esperienza e conoscenza adeguata nei seguenti campi:

- Sicurezza delle informazioni: networking, infrastrutture di rete, indirizzamento, architetture di elaborazione, gestione dei database, infrastrutture di sicurezza, endpoint management, strutture client-server, ecc.
- Monitoraggio e controllo: effettuazione delle operazioni di controllo, tramite strumenti automatici o mediante analisi manuale del corretto funzionamento degli apparati; controllo della corretta configurazione delle infrastrutture; identificazione e classificazione degli eventi in relazione alle tipologie di allarmi scatenati.
- Gestione degli incidenti: gestione delle emergenze, governo rapido ed efficace delle operazioni di contenimento degli incidenti di sicurezza in ambito IT, cooperazione con le altre linee di business.

I profili saranno corredati dalle necessarie certificazioni, in funzione dei ruoli svolti. Come regola generale, le risorse dovranno possedere alcune tra le seguenti tipologie di certificazioni, in base al ruolo ricoperto:

- Capo Progetto: PMP o Prince2;
- Specialisti di Governance: CISM, CRISC, ISO/IEC 27001 Lead Auditor;
- Technical Head e Security Architect: CISSP, CISA, CISM, ITIL, e certificazioni tecniche di prodotto;
- Specialisti di prodotto: altre certificazioni specialistiche di prodotto;

Le procedure di formazione e aggiornamento delle aziende del NewCo PSN assicurano l'allineamento delle conoscenze e delle competenze dei profili al mercato e la garanzia di formazione continua per far fronte al rischio di obsolescenza anche delle competenze stesse.

3.3 Processi di gestione della sicurezza

L'obiettivo della NewCo PSN è contrastare le minacce che possano mettere a repentaglio le informazioni delle Amministrazioni e l'erogazione dei servizi oggetto della fornitura. Per il raggiungimento di tale obiettivo, la NewCo si impegna a gestire la sicurezza delle informazioni garantendone la Riservatezza, l'Integrità e la Disponibilità attraverso il rispetto e l'attuazione delle Security Policy che saranno descritte nel Piano della Sicurezza.
In particolare, le regole, le procedure operative ed organizzative attuative delle suddette Security Policy saranno riportate in specifiche procedure di gestione della sicurezza IT conformi allo standard ISO/IEC 27002, in linea con quanto prescritto dall'Allegato A della Circolare AgID nr 1 del 14 giugno 2019 in tema di PSN nonché delle normative elencate nel § 3.1, tra cui si ricordano quelle inerenti la tutela dei dati personali e quelle applicabili agli Operatori di Servizi Essenziali (OSE) ed ai soggetti inclusi.

Tra queste procedure rientrano a titolo esemplificativo le seguenti:

- procedura per la classificazione delle informazioni;
- procedura per la gestione degli asset, ivi incluso quanto prescritto dal DPCM nr 131/2020 in materia di Perimetro di Sicurezza Nazionale Cibernetica, che richiede la comunicazione

all'autorità competente dell'Elenco dei Beni ICT inclusi nel perimetro e dell'Analisi del Rischio;

- procedura per il controllo degli accessi logici;
- procedura per la gestione della sicurezza fisica ed ambientale;
- procedura per la gestione dei cambiamenti;
- procedura per la gestione del back-up;
- procedura per la gestione dei log;
- procedura per la gestione delle vulnerabilità tecniche;
- procedura per la gestione della sicurezza della rete;
- procedura per la gestione della sicurezza nei processi di acquisizione, sviluppo e manutenzione dei sistemi. Con riferimento al processo di acquisizione si terrà conto anche di quanto prescritto dal DPR nr 54/2021 in materia di Perimetro di Sicurezza Nazionale Cibernetica e suoi regolamenti attuativi, che definiscono le procedure, modalità e termini di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di valutazione (CV);
- procedura per la sicurezza delle terze parti;
- procedura per la gestione degli incidenti di sicurezza, ivi incluso quanto prescritto dal DPCM n. 81/2021 in materia di Perimetro di Sicurezza Nazionale Cibernetica, che definisce le modalità di notifica degli incidenti aventi impatto sui Beni ICT perimetro al CSIRT Italia. In particolare, il decreto individua i tipi di incidenti cibernetici per i quali è obbligatoria la notifica al CSIRT Italia, dividendoli in due categorie sulla base della gravità dell'incidente stesso e stabilendo diverse tempistiche per la relativa notifica. Gli incidenti cibernetici che rientrano nei 19 tipi considerati meno gravi (categoria A) devono essere notificati al CSIRT entro 6 ore, mentre quelli che rientrano nei 6 tipi considerati più gravi (categoria B) entro un'ora, con l'obbligo di integrare tempestivamente quanto comunicato in caso di conoscenza di elementi aggiuntivi (salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa). Al contempo, è possibile notificare, su base volontaria, anche i tipi di incidenti non elencati nel decreto.

3.4 Tecnologie e Best Practices

Le tecnologie impiegate per garantire la protezione dei dati e per estensione delle infrastrutture a supporto dei servizi erogati saranno scelte con le garanzie di:

- allineamento con il mercato per l'adozione di tecnologie di sicurezza di tipo COTS o Open Source largamente diffuse e accreditate come leader di mercato allo scopo di massimizzare l'efficacia, la facilità d'uso e al contempo ridurre i rischi di lockdown tecnologico;
- riuso di esperienze già fatte con altri clienti nella stessa area di mercato o in aree affini;

- sistemi open che garantiscono la massima compatibilità con eventuali altre tecnologie IT e/o di sicurezza che potranno essere introdotte in seguito.

In fase di progettazione saranno garantite, secondo le principali best practice, la protezione delle infrastrutture IT e di rete, nonché la protezione delle informazioni in esse memorizzate, implementando le architetture e i controlli di seguito descritti.

L'implementazione delle best practice e dei controlli di sicurezza sarà parte integrante della realizzazione della sicurezza by design dei due centri Private Cloud. Per quanto riguarda il Secure Public Cloud ne sarà puntualmente verificato con il Cloud Provider l'utilizzo, ed eventualmente realizzati dei piani di conformità addizionali, se necessari.

Il PSN fornirà la **gestione della sicurezza** in accordo alle responsabilità tradizionalmente definite all'interno di tutti i modelli IaaS e PaaS previsti nel presente progetto, come riportato nella figura seguente:

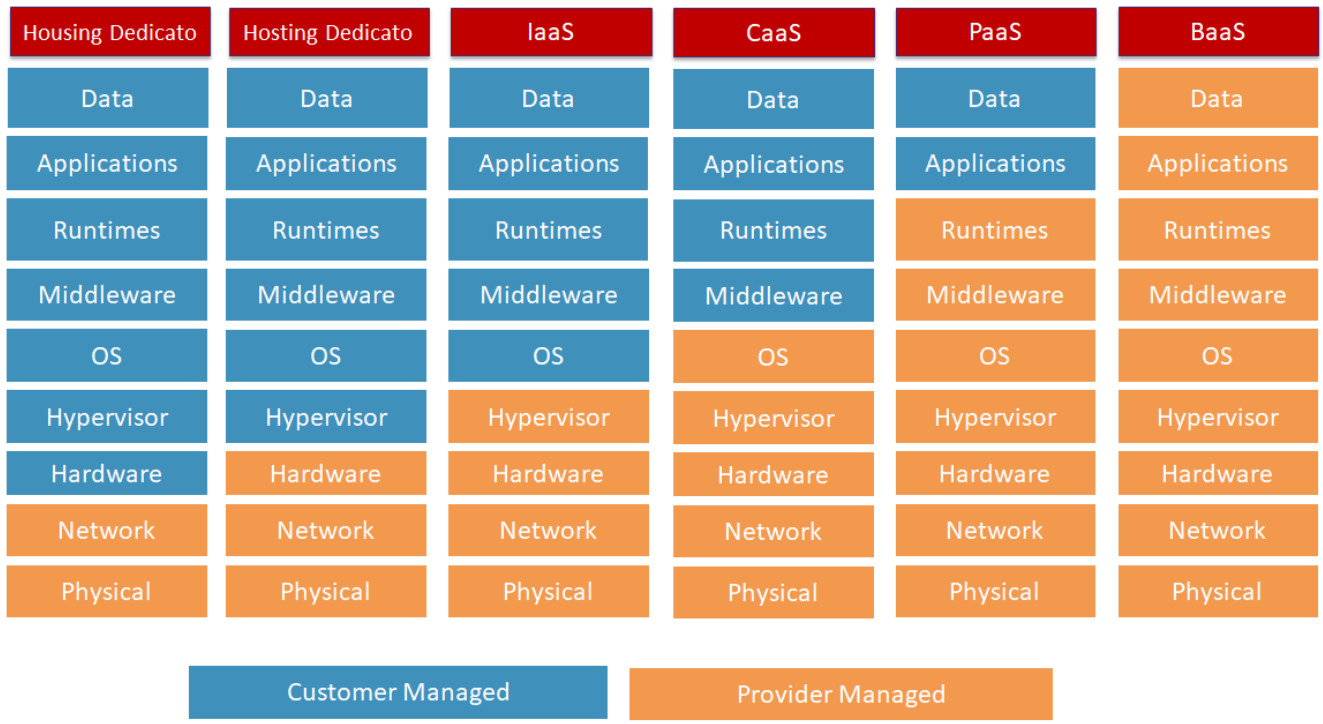


Figura 16: Gestione della Sicurezza

Nei paragrafi seguenti le componenti fondamentali di sicurezza che saranno implementate all'interno del PSN.

3.5 Infrastructure Security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.

La sicurezza delle infrastrutture è in carico al PSN, nei limiti di quanto espresso in Figura 15 – Gestione della Sicurezza.

Il Centro Servizi sarà realizzato prevedendo le seguenti soluzioni ed infrastrutture di sicurezza IT:

- **Segregazione degli ambienti**: soluzioni e procedure per garantire la segregazione degli ambienti elaborativi a seconda della categorizzazione e della rischiosità delle attività ivi condotte e del livello di criticità dei dati trattati, garantendo l'applicazione del principio di difesa in profondità. Sarà garantita la separazione fisica, di rete e logica in accordo ai criteri di classificazione identificati (rischiosità attività, dati trattati e difesa in profondità) e assicurata la relativa coerenza. Per i servizi di Housing e Hosting sarà realizzata la segregazione dei sistemi e delle reti a livello di tenant di tipo logico tramite VLAN e subnetting. Per i servizi XaaS sarà realizzata la segregazione dei sistemi e delle reti tramite tecnologie di Software Defined Network (SDN).
- **Accesso ai sistemi di elaborazione:** soluzioni I&AM per garantire che l'accesso verso gli ambienti elaborativi, con criteri di accesso restrittivi verso quelli più critici e rilevanti per la natura dei dati trattati, ad esempio accessibili attraverso macchine dedicate, collocate su una rete logicamente dedicata. Tali macchine non potranno essere utilizzate per altre attività e presenta configurazioni di sicurezza del tipo: accesso con autenticazione a due fattori, restrizioni delle attività rischiose (es. ricezione/invio di email), logging abilitato. Per i servizi di Housing, l'accesso ai sistemi di elaborazione è a carico dell'Amministrazione.
    - **Security logging:** soluzioni e procedure per assicurare la registrazione e la tracciabilità delle operazioni sui sistemi e le componenti di rete. Le soluzioni e le procedure adottate garantiranno che gli accessi degli utenti ai sistemi informativi siano sempre registrati in un apposito file di log di cui è necessario assicurare le caratteristiche di completezza, inalterabilità e possibilità di verifica della integrità delle registrazioni. I log saranno raccolti tramite uno strumento di log management ai fini di "audit", "prevention" e "detection" di minacce alla sicurezza dei dati, con inclusione di quelli personali. Tutti i dispositivi ed in particolare quelli che producono dati di tracciamento avranno l'orologio interno sincronizzato con i sistemi centralizzati (ad esempio connettendosi a GPS o NTP affidabili). Le relative connessioni saranno protette da interferenze e manomissioni. Per i servizi di Housing e Hosting il logging dei sistemi è a carico dell'Amministrazione, mentre quello degli apparati di rete è a carico del PSN.
- **Security Hardening:** Il Data Center prevede procedure di configurazione sicura dei sistemi in modo da minimizzare la superficie di attacco attraverso la rimozione dei servizi non strettamente necessari e per quelli rimanenti, assicurare che le parametrizzazioni di sicurezza siano correttamente implementate. Gli standard di Hardening saranno basati su fonti riconosciute, tra le quali, a titolo esemplificativo: www.nist.gov, www.sans.org e www.cisecurity.org, www.iso.org e i fornitori di prodotti. Per i servizi di Housing e di Hosting, l'Hardening dei sistemi di elaborazione è a carico dell'Amministrazione.
- **Sicurezza dei sistemi elaborativi:** Il Data Center sarà dotato di strumenti, procedure e personale qualificato per assicurare la protezione dei sistemi elaborativi tramite software di end point protection e end point detection & response. Per i servizi di Housing e Hosting

l'Hardening dei sistemi di elaborazione è a carico dell'Amministrazione. Per i servizi XaaS è a carico dell'amministrazione la protezione dei Sistemi Operativi in caso di IaaS, mentre è a carico del PSN nel caso di PaaS, CaaS e SaaS, nei limiti di quanto stabilito in Figura 15 Gestione della Sicurezza.

3.6 Network security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture, reti e archivi adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.

La sicurezza dell'infrastruttura di rete è a carico del PSN e include la sicurezza di tutti i servizi on top ai servizi Cloud, quali Help Desk e Contact Center, NOC, SOC e CERT, CMP, Portali di accesso e gestione, infrastruttura interna di amministrazione e gestione dell'infrastruttura del Cloud Center.

Il Centro servizi sarà protetto con tecnologie di protezione delle reti che includono quelle specificate di seguito.

- **Network Security:** strumenti, procedure e personale per gestire le richieste di definizione di regole di filtraggio del traffico IP (Network Firewall), con relativi workflow di approvazione e in maniera auditabile. Regolare review delle regole firewall deve essere garantita con periodicità di almeno 6 mesi.
- **NGFW e/o IDS/IPS:** strumenti NGFW e/o IDS/IPS allo stato dell'arte per controllare il traffico ingoing e outgoing dall'ambiente ospitato con relativi workflow di approvazione e in maniera auditabile. Regolare review delle regole di sicurezza deve essere garantita con periodicità di almeno 6 mesi.
- **Network Access Control (NAC):** strumenti di controllo e autenticazione degli endpoint che si connettono alla rete. Supporterà lo standard 802.1X e ulteriori meccanismi di autenticazioni (es. certificati digitali). Assicurerà controlli preventivi sulla sicurezza dell'host per la compliance dei dispositivi alle policy di sicurezza.
- **Accesso Zero Trust:** soluzioni e procedure che consentano l'accesso remoto tecnologie che implementano l'accesso mediante paradigma Zero Trust.
- **Web Application Firewall (WAF):** strumenti WAF allo stato dell'arte per controllare il traffico ingoing e outgoing dagli ambienti elaborativi. L'infrastruttura WAF sarà ridondata ed in alta affidabilità. Le policy di detection dei WAF saranno definite in relazione alle funzionalità applicative e le vulnerabilità applicative di riferimento (es. OWASP) e saranno regolarmente aggiornate in relazione alle evoluzioni dell'applicazione che protegge.
- **E-mail & Web Security**: strumenti di protezione e-mail e Web (Secure E-mail Gateway e Secure Web Gateway) per la protezione del traffico e-mail e web relativamente al personale del centro, con relativi workflow di approvazione e in maniera auditabile. Sarà assicurata la disponibilità di strumenti di contrasto avanzato di APT e minacce zero-day tramite l'utilizzo di funzionalità di sandboxing.
- Tutti i dispositivi saranno configurati per inviare i log delle attività alla piattaforma di log management. I log saranno raccolti tramite uno strumento di log management ai fini di

"audit", "prevention" e "detection" di minacce alla sicurezza dei dati, con inclusione di quelli personali.

3.7 Data Security

La NewCo PSN assicurerà l'integrità, la riservatezza e la disponibilità delle informazioni attraverso misure di protezione delle infrastrutture, reti e archivi adeguate alla criticità dei servizi oggetto di tale progetto, erogati nelle diverse modalità.

Il Centro servizi sarà protetto con tecnologie di protezione avanzata dei dati che includono:

- **Data discovery and classification:** Il Centro Servizi per assicurare una maggiore protezione dei dati disporrà di soluzioni, procedure e personale assicurano un presidio di data discovery e di data classification, contribuendo alla Data Governance. Attraverso gli strumenti e le procedure di data discovery si mirerà a scoprire dati strutturati e non in modo che siano classificati e protetti.
- **Data at rest encryption:** Il Centro Servizi adotterà strumenti e procedure per garantire la protezione dei dati quando salvati sui dischi in uso per lo storage dei dati. La cifratura dei dischi sarà implementata in accordo con le principali best practice e standard (es. NIST Special Publication 800-57 Part 1, FIPS, PCI DSS).
- **Data in transit protection:** Il Centro Servizi impiegherà strumenti e procedure per assicurare la protezione della riservatezza dei dati quando in transito, con particolare attenzione alla comunicazione via reti pubbliche. La cifratura delle comunicazioni includerà diversi meccanismi riconosciuti come standard di settore, come ad esempio IPSEC, TLS.
- **Database encryption:** Il Centro Servizi per assicurare una maggiore protezione dei dati a livello di archiviazione fisica, ossia dati archiviati e file di registro, impiegherà strumenti e procedure per assicurare la cifratura dei database. La soluzione potrà assicurare la crittografia in tempo reale dei database senza dover modificare le applicazioni che li usano.
- **Data masking:** Il Centro Servizi al fine di assicurare che i dati più critici siano solo disponibili in ambiente di produzione e che siano rispettati i vincoli di minimizzazione dei dati utilizzerà soluzioni e procedure atte a creare copie sicure e protette dei dati mediante l'anonimizzazione e la crittografia delle informazioni che potrebbero minacciare la privacy, la sicurezza o la conformità dei dati.

Le aree di controlli tecnologici che saranno implementate all'interno del Centro Servizi saranno a copertura delle aree descritte nei seguenti paragrafi (SOC/CERT), in cui viene dettagliato il relativo servizio.

3.8 SOC

Per realizzare i servizi erogati dal SOC, la NewCo PSN metterà a disposizione un Security Operation Center dal quale saranno erogati i servizi di gestione operativa della sicurezza. La Control Room del SOC sarà localizzata esternamente ai centri servizi del PSN. L'infrastruttura da gestire, che implementa i controlli tecnologici che proteggono le infrastrutture a supporto dei servizi saranno

invece ospitate all'interno dei Data Center. I servizi SOC saranno disponibili in orario continuato (8x5) più reperibilità.

Il servizio di Security Monitoring sarà disponibile in finestra oraria estesa (24x7).

Dal SOC saranno erogati i servizi di gestione delle piattaforme di sicurezza utilizzate all'interno dei Centri Servizi, descritti nei seguenti paragrafi.

3.8.1 End Point Protection

La NewCo PSN disporrà di strumenti, procedure e personale qualificato per assicurare la gestione della sicurezza degli End Point utilizzati per lo svolgimento delle attività lavorative e, ove applicabile per i servizi di hosting e X-aaS, per tutte le funzionalità necessarie per l'erogazione degli stessi.

Le tecnologie a supporto del servizio di gestione della sicurezza degli End Point avranno le seguenti funzionalità:

- Crittografia dei dischi;
- Software di protezione antivirus (AV), costantemente aggiornato, e con inibita, salvo impossibilità tecniche, la possibilità di disabilitare l'antivirus da parte degli utenti;
- Software di Data Loss Prevention, per identificare, monitorare e proteggere i dati in uscita dagli endpoint attraverso l'intercettazione e il blocco;
- Software di protezione avanzata denominato Endpoint Detection & Response che operi in modo integrato con le difese antivirus (AV) e metta a diposizione funzionalità di (a) analisi del comportamento e machine learning per bloccare attività malevole, (b) gestione degli indicatori di compromissione (IOC), e (c) produzione delle evidenze per l'analisi forense;
- Personal firewall e device control;
- Gestione dei dispositivi mobili attraverso soluzione di Mobile Device Management (MDM).
- File Integrity Monitoring

Sono esclusi servizi di End Point Security degli endpoint interni ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. Macchine Virtuali).

3.8.2 Identity and Access Management

La NewCo PSN disporrà di strumenti, procedure e personale qualificato per il governo degli accessi logici, la gestione e il controllo degli accessi privilegiati ai sistemi, meccanismi di autenticazione semplice e multifattoriale e servizi di federazione delle identità.

Il SOC dovrà erogare servizi di sicurezza inerenti alla gestione degli accessi logici che includano:

- **Identity and Access Governance:** Il Data Center avrà strumenti, procedure e personale qualificato per assicurare la gestione e il controllo del ciclo di vita delle identità logiche. Dovranno essere presenti procedure e meccanismi di provisioning e deprovisioning delle

utenze sui diversi target e, ove possibile, meccanismi di automazione delle relative attività. Dovrà essere assicurata l'univocità degli account e le relative password devono essere individuali. Dovranno essere presenti procedure e meccanismi di richiesta di accesso logico con relativi workflow di approvazione. Sarà assicurata la cessazione delle identità logiche non appena non vi siano più le condizioni che ne rendono necessaria la definizione (es. cessazione del rapporto di lavoro). Dovranno essere presenti procedure e meccanismi atti ad effettuare la revisione periodica degli accessi per assicurare che le abilitazioni rilevate siano in linea con il ruolo di business.

- **Privileged Access Management:** Il controllo delle utenze privilegiate attraverso la memorizzazione delle relative credenziali in vault logici e la registrazione delle sessioni amministrative verso i target. Saranno presenti procedure e meccanismi di provisioning e deprovisioning delle utenze privilegiate con relativi workflow di approvazione. Le attività di gestione delle utenze privilegiate dovranno essere registrate e le registrazioni collezionate centralmente presso un sistema di analisi e correlazione eventi (SIEM). La infrastruttura della soluzione di gestione e controllo delle utenze privilegiata dovrà garantire ridondanza e alta affidabilità.
- **Authentication Management:** Il Data Center avrà strumenti, procedure e personale qualificato per assicurare la gestione delle credenziali di accesso in linea con gli standard e le best practice di settore.
- **Identity Federation services:** Il Data Center avrà strumenti per assicurare la federazione delle identità attraverso meccanismi standard e industry best practice (es. SAML e OAUTH).
- **Multi-factor Authentication:** Il Data Center sarà dotato di strumenti, procedure e personale qualificato per assicurare che l'accesso logico possa avvenire con meccanismi aggiuntivi alla password in linea con la definizione di 2 factor authentication definita dagli standard e dalle best practice di settore.

L'erogazione del presente servizio è prevista per il funzionamento del presente progetto in favore dei clienti che usufruiscono dei servizi di Hosting e XaaS. Sono esclusi servizi di I&AM per le utenze interne ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. account e/o user su Macchine Virtuali).

3.8.3 Key Management

La NewCo PSN assicurerà la gestione delle chiavi crittografiche e dei certificati digitali relativamente ai servizi erogati in modalità Hosting e XaaS.

Tale servizio sarà conforme a quanto indicato nelle pubblicazioni NIST 800-57.

Il SOC garantirà soluzioni, procedure e personale qualificato per la gestione delle chiavi crittografiche simmetriche e asimmetriche in accordo con le principali best practice e standard (es. NIST Special Publication 800-57 Part 1, FIPS, PCI DSS).

Il servizio avrà le seguenti caratteristiche:

- Le procedure di gestione delle chiavi dovranno assicurare il dual control e lo split knowledge, oltre che la piena tracciabilità nell'uso e nella gestione delle chiavi, in linea con gli standard e le best practice di settore (es. NIST, PCI DSS).
- Le chiavi di cifrature conservate dentro key store cifrati (e.g., a FIPS 140-2 Level 3 compliant hardware security module).
- I ruoli e le responsabilità dei custodi delle chiavi crittografiche saranno documentati e conosciuti
- Il personale incaricato opererà in piena segregazione organizzativa, fisica, operativa
- Le procedure dovranno regolamentare l'intero ciclo di vita delle chiavi, ossia la gestione della generazione, scambio, archiviazione, utilizzo, crypto-shredding (distruzione) e sostituzione delle chiavi
- I certificati digitali saranno gestiti attraverso specifica piattaforma che comprende il monitoraggio delle scadenze.

L'erogazione del servizio è prevista per il funzionamento del presente progetto e in favore dei clienti che usufruiscono dei servizi di Hosting e XaaS. É esclusa la gestione delle chiavi interne ai servizi di Hosting, e XaaS medesimi di gestione delle Amministrazioni (es. certificati SSH su Macchine Virtuali).

3.8.4 Security Platform Management

Il SOC garantirà il servizio di Security Platform Management che si applica alle seguenti piattaforme:

- End Point Security;
- I&AM;
- Key Management;
- Network Firewall;
- Next Generation Firewall e IDS/IPS;
- Web Application Firewall;
- Secure E-mail Gateway;
- Secure Web Gateway;
- Data Loss Prevention;
- SIEM/SOAR;
- Network & Zero Trust Access Control.

Il servizio assicura:

- La gestione di tutte le piattaforme di sicurezza;
- La manutenzione evolutiva e correttiva delle piattaforme di sicurezza, compresi upgrade e applicazione delle patch e hotfixes;

- La verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma.

3.8.5 Security Policy Management & Enforcement

Il SOC garantirà il servizio di security Policy Management & enforcement, assicurando:

- La gestione di tutte le richieste di implementazione/modifica policy di sicurezza sulle piattaforme di sicurezza inclusive di:
  - Network Firewall;
  - Next Generation Firewall e IDS/IPS;
  - Web Application Firewall;
  - Secure E-mail Gateway;
  - Secure Web Gateway;
  - Data Loss Prevention;
  - SIEM/SOAR;
  - Network & Zero Trust Access Control.
- Il controllo dell'efficacia delle contromisure di sicurezza attive sul dispositivo.

3.8.6 Log Management

Il SOC garantirà il servizio di Log Management tramite un'infrastruttura di log collection & archiving.

I log saranno raccolti in modalità agent based or agentless e archiviati all'interno di una piattaforma di log management e protetti da modifica, cancellazione e distruzione, nonché accessibili solo da personale autorizzato. I sistemi saranno configurati per evitare la sovrascrittura degli eventi. I log e gli eventi di sicurezza saranno resi disponibili e trasferiti alla infrastruttura preposta alla loro analisi e correlazione. La ritenzione dei file di Log rispetterà le normative applicabili.

Il SOC si occuperà della gestione della piattaforma e di:

- assicurarsi della corretta raccolta dei log dalle sorgenti in perimetro;
- effettuare la verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma;
- verificare la corretta archiviazione dei log;
- rendere disponibili i log su richiesta;
- supportare procedure e sessioni di audit, nonché attività di gestione di incidenti di sicurezza;

- effettuare la verifica ed il monitoraggio degli eventi e degli incidenti per assicurare il corretto funzionamento di tutte le componenti della piattaforma.

3.8.7 Security Monitoring

La NewCo PSN erogherà servizi che mirano al monitoraggio del livello di sicurezza delle informazioni per la pronta rilevazione di incidenti o anomalie di sicurezza.

Saranno utilizzati strumenti, procedure e personale qualificato per assicurare il monitoraggio in tempo reale del livello di sicurezza delle infrastrutture, rilevare ed eventualmente investigare le anomalie di sicurezza e gestire in caso di necessità la risposta alle gravi minacce e agli incidenti.
Il team sarà composto da analisti e specialisti di sicurezza suddivisi in 1° e 2° livello e organizzati per assicurare il presidio continuativo e l'attivazione del personale specialistico in reperibilità negli orari extra lavorativi.

Il presidio di primo livello sarà organizzato in combinazione con altre funzioni di gestione operativa se adeguate in termini di strumenti e personale qualificato.

Al fine di garantire efficacia per il rilevamento e monitoraggio degli incidenti di sicurezza, il SOC utilizzerà strumenti di **Security Information and Event Management (SIEM).** Tale strumento consente l'analisi e la correlazione degli eventi di sicurezza per garantire la individuazione di eventi sospetti o anomali. Tale piattaforma concentrerà le registrazioni di sicurezza originate dalle soluzioni di sicurezza e dall'intera infrastruttura. Specifiche dashboard ed allarmi saranno rese disponibili per assicurare il monitoraggio della sicurezza della intera infrastruttura, includendo applicazioni, sistemi e reti. Lo strumento raccoglierà i log dalla piattaforma di log management o direttamente dai sistemi di elaborazione e dalle piattaforme di sicurezza.

3.9 CERT

Per realizzare i servizi erogati dal CERT la NewCo PSN metterà a disposizione un CERT esterno dal quale saranno erogati i servizi di sicurezza reattivi e proattivi. Anche la control room del CERT sarà localizzata esternamente ai centri servizi del PSN. L'infrastruttura da gestire, che implementa i controlli tecnologici che proteggono le infrastrutture a supporto dei servizi saranno invece ospitate all'interno dei Data Center. I servizi CERT saranno disponibili in orario lavorativo 09.00-18.00 dal lunedì al venerdì, garantendo reperibilità nel restante periodo.

La NewCo PSN assicurerà la risposta agli attacchi di tipo cibernetico attraverso strumenti, procedure e personale focalizzati alla valutazione degli scenari di minaccia, la rilevazione degli attacchi e il coordinamento delle azioni di risposta agli incidenti di sicurezza tramite una struttura dedicata e organizzativamente separata da quelle di gestione (IT, SOC).

Per assicurare un'appropriata segregazione dei ruoli, questo team non potrà includere il personale operativo che ha in gestione l'infrastruttura da monitorare, assicurando la necessaria terzietà del controllo.
Al fine di garantire efficacia nella pronta individuazione delle minacce e nella risposta agli incidenti di tipo cibernetico, il CERT del Data Center dovrà avere le seguenti caratteristiche minime:

- avere relazioni formali e riconosciute con CERT rilevanti (es. Polizia Postale/CNAIPIC, CSIRT Italia e CERT AgID);
- dotarsi di procedure di cyber security incident che in linea con gli standard e le best practice di settore includano gli step necessari alla classificazione, contenimento, analisi delle cause, e radicamento e notifica verso le Autorità, oltre che raccolta delle eventuali evidenze forensi;
- promuovere campagne di awareness e prevedere simulazioni in ambito sicurezza cibernetica allo scopo di valutare la readiness nella risposta a minacce e incidenti siffatti.

In questo ambito rientrano i servizi descritti nei successivi paragrafi.

3.9.1 Threat Hunting

Il CERT per rilevare segnali deboli che possono indicare la compromissione delle infrastrutture, degli ambienti elaborativi o la compromissione di un utente tramite una capacità di Threat Hunting, che permette di indentificare comportamenti anomali o associati a tecniche tattiche e procedure note di attacco.

3.9.2 Threat intelligence & Infosharing

La NewCo PSN sfrutterà servizi avanzati di Threat intelligence & Information Sharing e adotterà strumenti, procedure e personale per assicurare competenze predittive in ambito sicurezza cibernetica.

Nel farlo verranno attivati servizi di intelligence che consentano di:

- scambiare informazioni in forma anonimizzata su nuove tecniche di attacco (TTPs) e scenari di minaccia;
- scambiare informazioni in forma anonimizzata, anche in forma di IOC (Indicator of Compromise) su incidenti di sicurezza cibernetica occorsi;
- ricevere notifiche e allarmi su minacce di Cyber (es. zero-day, campagne di malware, pandemie digitali, attori e incidenti)

Per verificare in maniera capillare e tempestiva la presenza di indicatori di compromissione, sarà necessario dotare il Centro Servizi di strumenti di IoC automation basati sull'integrazione di:

- piattaforme open-source (es. MISP Open Source Threat Intelligence and Sharing Platform – precedentemente nota come Malware Information Sharing Platform);
- software di protezione avanzata denominato Endpoint Detection & Response come descritto nel paragrafo 3.8.1End Point Protection;
- strumenti di log management in grado di correlare ed allarmare la presenza di SOC sia in real-time che sullo storico dei log con congrua profondità.

3.9.3 Security Testing & Vulnerability Management

I Data Center avranno strumenti, procedure e personale per gestire le attività di testing delle infrastrutture, valutarne i relativi risultati, identificare e indirizzare le strategie di mitigazione.

Il Data Center utilizzerà strumenti, procedure e personale per gestire le attività di testing delle infrastrutture e valutarne i relativi risultati. Dato che un'adeguata protezione dalle minacce di sicurezza necessita di un approccio sistematico e continuativo, sarà prevista l'esecuzione periodica di sua serie di verifiche e test di sicurezza (Vulnerability Assessment e Penetration Test), al fine di mantenere i livelli di rischio residuo in linea con i requisiti (es. OWASP).

Il Data Center garantirà una adeguata copertura delle attività di testing, prevedendo come requisiti minimi:

- Vulnerability assessment almeno trimestrali dall'esterno e dalle reti interne in corrispondenza dei front end;
- Penetration test infrastrutturale dall'esterno con cadenza semestrale;

Al fine di rimediare le eventuali vulnerabilità riscontrate il Data Center adotterà le procedure di gestione delle vulnerabilità in linea con le best practices di settore e i principali standard di sicurezza (es. CIS, SANS, PCI DSS).

Queste prevedono che la classificazione delle vulnerabilità avvenga secondo standard internazionali (es. CVSS) e le attività di rimedio siano proporzionate al livello di esposizione al rischio introdotto dalle vulnerabilità.

3.9.4 Incident Response

L'Incident Response è un servizio erogato dal CERT in risposta agli incidenti di sicurezza. La risposta sarà attivata dai processi di monitoraggio SOC, dalla verifica di segnalazioni di Threat Intelligence o da richiesta interna o di terze parti. Il servizio prevede un'investigazione di dettaglio che permette di definire la migliore strategie di risposta e coordinare i vari gruppi necessari per indirizzare la parte di rimedio.

Le attività principali sono atte a isolare i sistemi compromessi, preservare e non alterare le evidenze digitali, verificare l'occorrenza e la causa ultima dell'evento analizzato e indicare le corrette metodologie per eradicare la minaccia e ripristinare i sistemi effetti. A completare il servizio si effettua attività di malware analysis e/o analisi forense ove richiesta.

Per realizzare il servizio di security monitoring, sarà introdotta anche una piattaforma **SOAR** in uso dal CERT, per l'automazione delle procedure di security incident management e l'integrazione delle tecnologie utilizzate per la detection e la reazione.

4 Infrastruttura IT e Network

I Servizi elencati nel *§. 1.4 Oggetto della Fornitura* saranno erogati dal Centro Servizi della NewCo PSN in modalità "run", a meno del servizio di Migrazione che sarà attivato "una tantum". La finestra temporale di erogazione dei servizi in modalità "run" è 24H (00:00 – 24:00) per 365 giorni l'anno.

Dal momento della stipula del contratto, i Servizi verranno attivati e resi disponibili alle PA che li richiedano secondo quanto indicato nel presente documento, fermo restando che tutti i servizi, o parte di essi, ovvero anche uno solo di essi, potranno subire variazioni in aumento o in diminuzione.

In caso di guasto, la NewCo PSN è tenuta a ripristinare la perfetta funzionalità e la piena disponibilità dei Servizi oggetto di Fornitura, garantendone i tempi di ripristino secondo quanto previsto dagli indicatori di qualità definiti nell'allegato 1 del documento di "Specificazione delle caratteristiche del Servizio e della Gestione".

I Servizi di Infrastruttura IT consistono nella messa a disposizione, da parte della NewCo PSN, di tutti gli apparati hardware e software infrastrutturale necessari a garantire gli elevati standard qualitativi in termini di affidabilità e disponibilità nel rispetto dei requisiti indicati di seguito al ***paragrafo 4.1 Apparati Hardware e software infrastrutturale***.

La NewCo PSN si farà carico di tutte le attività di progettazione e set up dell'Infrastruttura IT, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

Di seguito sono riportate le infrastrutture IT impiegate per le diverse modalità di erogazione (Housing, Hosting e IaaS):

- **Server fisici**: l'infrastruttura della PA sarà ospitata esclusivamente su server **dedicati** tra PA che ne richiedano l'erogazione in tale modalità. L'erogazione del presente servizio è prevista nella sola modalità Hosting.
- **Server virtuali**: l'infrastruttura della PA virtualizzata sarà ospitata esclusivamente su server **condivisi** tra PA che ne richiedano l'erogazione in tale modalità. L'erogazione del presente servizio è prevista nella sola modalità IaaS
- **Storage**: l'insieme di dispositivi Hardware e Software messi a disposizione per l'immagazzinamento permanente dei dati. L'erogazione del presente servizio è prevista nelle modalità Hosting e IaaS.

4.1 Apparati Hardware e software infrastrutturale

4.1.1 High Level Design dell'architettura

Il modello di riferimento prevede una piattaforma Cloud che grazie a un global control plane consentirà di erogare servizi da diverse Regioni (Region) e relative zone di disponibilità (Availability Zones - AZ) in territorio italiano. Ciò consentirà quindi ad ogni PA di abilitare servizi aggiuntivi per la protezione di sistemi e dati, in modo da realizzare configurazioni in Business Continuity e/o in Disaster Recovery.

La singola PA potrà attingere a servizi Cloud disponibili in una qualunque Region e relativa AZ e potrà interconnetterli tra di loro grazie ad un Network Layer logico, unico e trasversale, realizzato sul paradigma del Software Defined Network.

Inoltre, la Cloud Platform avrà un «connettore» diretto verso i Cloud Service Provider *Hyperscaler* (Google, Microsoft, Oracle): tale connettore garantirà una funzione di Cloud Services Gateway per l'interfacciamento diretto e privato verso i servizi Cloud degli *Hyperscaler* (Service Brokering) da parte dei workload della PA ospitati nel Cloud PSN.

L'infrastruttura Cloud sarà ospitata all'interno di **4 Data Center distribuiti sul territorio italiano,** allestiti in una configurazione di **doppia *Region* (2 DC + 2 DC)**, e quindi ciascuna ridondata con una coppia di zone di disponibilità in alta affidabilità. I data center sono dotati di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire i massimi standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti.

La configurazione infrastrutturale è quindi completamente ridondata grazie alla suddivisione di ognuna delle due Region (Nord e Sud, distanti tra loro centinaia di chilometri) in *dual-AZ* (Availability Zone), cioè una coppia di Data Center in configurazione di business continuity, distanti tra loro diverse decine di chilometri in linea d'aria. In particolare, le due AZ sono interconnesse grazie ad un backbone proprietario che garantisce a sua volta completa ridondanza, latenza trascurabile e connettività privata, tale da caratterizzare la coppia logicamente come un unico Data Center virtuale (*Software Defined Data Center*).

Anche le Region sono interconnesse attraverso lo stesso backbone proprietario e da un Network layer in grado di consentire un'architettura di rete logica flessibile, Software Defined, che garantisca la mobilità dei carichi applicativi e l'alta affidabilità intrinseca delle soluzioni Cloud.

All'interno di una zona di disponibilità dunque i workload vengono distribuiti in maniera trasparente e la configurazione di HA (High Availability) consente di realizzare la continuità di servizio infrastrutturale (Business Continuity) tra i due data center della stessa Region (vedi documento specifico "*Specificazione delle caratteristiche del servizio e della gestione PSN_v11*" per le caratteristiche del servizio DR/BC offerto). Di fatto, grazie a questa configurazione di base, la piattaforma Cloud prevederà la distribuzione anche dei dati nelle due zone di ogni singola Region. Questa configurazione è possibile grazie alla distribuzione dello storage space (individuato in tecnologie di Storage Array tra le migliori disponibili sul mercato IT) all'interno delle due AZ e quindi grazie alla continuous data replication del servizio prescelto da ogni singola PA. In tal modo, qualora una singola PA decidesse di avvalersi della ridondanza completa della sua infrastruttura (fisica o virtuale che sia) potrà far leva sulla configurazione in HA della piattaforma Cloud e costruire così delle soluzioni di DR/BC.

La specificità della piattaforma Cloud, grazie al backbone proprietario di interconnessione delle due AZ costituenti ogni singola Region, permetterà la replica sincrona/asincrona dei dati tra i sistemi Storage Array costituenti lo Storage Layer.

In tale contesto operativo, la singola PA potrà beneficiare quindi della capacità intrinseca della piattaforma Cloud di reagire ad eventi disastrosi rendendo possibile la riattivazione dei workload all'interno di una delle due AZ o su una Region diversa. La ripartenza dei workload protetti dalla soluzione di DR/BC attivata, consentirà poi alla singola PA, in modo del tutto autonomo, la gestione del riavvio di ogni singola applicazione, secondo i propri piani di DR o di BC.

In caso di necessità, inoltre, la piattaforma Cloud prevede anche la disponibilità di backup di singoli componenti del workload della PA e dei relativi dati e, per protezione ulteriore, gli stessi backup possono essere trasferiti da una Region all'altra in modo tale che vi sia sempre una copia del dato disponibile in una delle due Region, al fine di poter avviare una restore in caso di necessità. Questa possibilità può essere utilizzata inoltre anche per esigenze di "*offsite vaulting*", ovvero per proteggere gli archivi di backup da eventi di disastro, replicandoli su una Region diversa (es. archivi di dati di cui occorra garantire la disponibilità a lunga conservazione per disposizioni normative): mentre le soluzioni di DR/BC si focalizzano sulla ripartenze dei servizi a fronte di eventi di disastro, e quindi sui dati correnti delle relative applicazioni, l'offsite vaulting si occupa quindi della protezione degli archivi di dati a lunga retention.

Le soluzioni tecnologiche in ambito Network WAN infine, garantiscono gli accessi remoti ai siti da parte di ogni singola PA e l'interconnessione fra i siti stessi. La piattaforma Cloud è quindi da intendersi come geograficamente distribuita e in grado di reagire a diverse situazioni di disservizio che dovessero generarsi durante il normale esercizio operativo.

Grazie a queste predisposizioni e configurazioni si potrà garantire, in base alle caratteristiche del servizio Cloud prescelto da una PA, la conformità a valori di RTO (Recovery Time Objective) e di RPO (Recovery Point Objective) per l'infrastruttura configurabili a seconda dell'esigenza, fino ai valori più stringenti disponibili e riportati nella seguente tabella:

RTO	RPO
30 minuti	**1 minuto**

In caso di soluzioni di continuità su Region distinte, ad esempio per implementazione di scenari di Disaster Recovery in grado di proteggere da eventi disastrosi come catastrofi naturali, la piattaforma Cloud sarà in grado di garantire valori di RTO e RPO almeno pari a:

Scenario	RTO	RPO
DR sito infrastrutturale	**4 ore**	**30 minuti**

La soluzione di DR resa disponibile prevede la possibilità di abilitare la configurazione di matrici di replica full-mesh tra tutti i DC costituenti le differenti Region. Ciò garantisce ad ogni PA la possibilità di scegliere di volta in volta la collocazione dei servizi più adatta alle proprie esigenze di workload (es. per prossimità geografica all'utenza, ecc) e delle relative istanze di replica.

4.1.2 Componente server

Il modello di architettura PSN si pone come obiettivo quello di essere standard dal punto di vista del Design architetturale a prescindere dal modello di servizio/offerta da erogare.
Basandosi su sistemi IT di tipo Blade Server configurabili tramite applicazione di Profili Logici predisposti per ogni esigenza in base al modello di erogazione del servizio/offerta, i singoli Blade server di tipo StateLess vengono profilati all'occorrenza sia dal punto di vista della configurazione HW che dell'OS/Hypervisor da installare per l'utilizzo finale.

Tutto questo è possibile grazie all'elevata standardizzazione e integrazione con il Network Layer e gli automatismi del Delivery automatico del Cloud Management Platform (CMP) che quindi consentono l'attivazione di server sia HW che virtuali.
Quindi, una volta effettuato l'iniziale Design Architetturale, integrati i sistemi Blade Server col Network Layer e con il CMP, non vi sarà alcun'altra progettazione da eseguire se non attivare, logicamente, nuovi profili di servizio per gli stateless system disponibili.

Il modello di architettura della NewCo PSN si propone come soluzione "**open**": architettura senza alcun tipo di **vendor Lock-In** e aperta alla potenziale creazione di tutte le possibili piattaforme progettate per l'erogazione di servizi ICT (*evitando di fatto l'acquisto di hardware ad hoc per ogni piattaforma di erogazione di un determinato servizio per il cliente finale*).

Il modello architetturale dell'Erogatore minimizza l'effort in termini di costi e tempi inerenti la Site Preparation perché la sua realizzazione è richiesta solo all'inizio («**one shot**»), durante la prima installazione del modello architetturale con i server di tipo Blade System e riutilizzata senza variazione alcuna per l'attivazione di nuovi Server Blade.

Dato l'utilizzo di Blade Server System ad alta standardizzazione, sarà possibile anche prevedere un preliminare predisposizione di spazi attrezzati nel DC al fine di ospitare nuovi Blade Server System di fatto riducendo il tempo necessario alle attivazioni di nuovi POD di erogazione di fatto migliorando il Time To Market per l'offerta di servizi ai clienti finali.

Eventuali esigenze di scalabilità dei Blade Server System, già installati in un DC, in termini di aggiunta banda di Uplink verso LAN e SAN, si riducono alla sola predisposizione di nuovi cablaggi in fibra ottica partendo da predisposizioni e configurazioni già create in precedenza e quindi di fatto semplificando anche questo eventuale insieme di attività.

La infrastruttura di computing sarà quindi basata su Blade System modulari che possano scalare orizzontalmente con la sola aggiunta di componenti Chassis e Blade Server in quanto la connettività LAN/SAN sarà predefinita e predisposta all'atto dell'attivazione e installazione del PoD (Point of Delivery).

La configurazione minima del Blade System avrà connettività LAN con multi interface da 10-100Gbps e SAN con multi interface 16-32Gbps.

Il sistema Blade Server System garantisce no SPOF e in particolare:

- alimentazione/alimentatori ridondati e di tipo hot-plug
- sistema di raffreddamento ridondato e di tipo hot-plug
- ridondanza di ogni modulo HW costituente lo Chassis ospitante i Blade Server così come tutto il Blade Server System
- Chassis/Blade Server Power Management (IPMI Enabled)
- HW/Chassis Management Module dell'intero Blade System ridondato e con connessione LAN Out of Band (ridondante) che consenta la completa configurazione/monitoraggio del sistema da remoto

Ogni Blade Server installabile e configurabile nel Blade System disporrà di:

- Minimo 2 socket CPU (CPU Intel o AMD con opzioni di risparmio energetico)
- Configurazione con almeno 16 core e multithreads enabled (parametri minimi: 2.5GHz/20-core/150W)
- Minimo 256GB di RAM e fino a 1TB di RAM

4.1.3 Componente storage

L'infrastruttura Storage prevista nell'architettura proposta è basata su Storage Area Network (SAN) fully redundant che consente connettività diretta Fiber Channel (FC) verso gli Storage Array Enterprise dai quali configurare storage space utile alla configurazione dei Blade Server (con relativo OS/Hypervisor).

La infrastruttura storage è in grado di erogare **80 PetaByte** e di scalare orizzontalmente in base alle esigenze dei clienti e delle relative infrastrutture durante tutto il loro ciclo di vita.
Il dato capacitivo si riferisce alla somma tra il dato live e la sua replica e la soluzione dovrà prevedere almeno il 20% di disco altamente prestazionale.

L'architettura storage infatti è in grado di garantire configurazione di tipo High Availability (HA) tra DC della stessa Region e abilitante al servizio di Disaster Recovery (DR) tra differenti Region con diversi SLA RTO/RPO disponibili (DRaaS).

L'architettura storage inoltre potrà erogare le seguenti modalità di servizio:

- Encryption;
- Configurazione "recovery automatico" sui due siti (HA);
- Thin Provisioning;
- Snapshot manager;
- Replica a tre siti (HA+DR);
- Automated Tiered anche su sito secondario;
- Connettività 32Gbps;
- Possibilità di passare da modalità sincrono ad asincrono (e viceversa) in maniera non distruttiva;
- Gestione, monitoraggio, reportistica, chargeback e storicizzazione delle performance.

4.1.4 Piattaforme software infrastrutturale

L'architettura di Blade System per il computing layer sarà disponibile per poter configurare sia Bare Metal Server con relativo OS (Microsoft Windows Server e/o Linux in different revision) sia Hypervisor (VMware e/o Red Hat Enterprise Virtualization e/o Oracle VM).

In tal modo sarà possibile andar a definire per ogni cliente il disegno architetturale voluto e necessario per garantire migrazione del workload preesistente presso i DC e ottimizzazione delle configurazioni grazie alla possibilità di consolidamento tecnologico su Blade System di nuova generazione e con capacità computazionali allineate agli ultimi rilasci tecnologici.

4.1.5 Backup standard

La NewCo PSN renderà disponibile un'infrastruttura Hardware e Software e un insieme di Standard e Linee Guida, comuni a tutti i DC di Servizio, per l'effettuazione delle attività di Backup e Restore.

Il servizio sarà reso disponibile attraverso un'unica console centralizzata dalla quale è possibile gestire la protezione dei propri dati attraverso un backup efficace e sicuro con un Restore rapido. Tale console consente la gestione in piena autonomia (in modalità self managed) della protezione dei dati permettendo quindi l'esecuzione di jobs di backup e restore dei svariati contesti (filesystem, virtual machine, database and application, posta elettronica, ecc) del cliente in modo efficace e sicuro.

I contesti da proteggere a cui è applicabile tale soluzione possono essere di varia tipologia (Files, VM, Container (k8), tutti i principali database come SAP-HANA, Exchange, SQL, Oracle, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, o i principali PaaS).

Il servizio garantisce al Cliente totale autonomia per il salvataggio dei propri dati e 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.

Il servizio si basa su dei backup server che coordinano ed eseguono tutte le operazioni di backup e remote vaulting. Sulla base delle schedulazioni pianificate, il backup server esegue i jobs di backup. In particolare, il Backup server avvia, sulla base delle schedulazioni programmate, la connessione tra gli agent presenti sui sistemi (Sistemi operativi o hypervisor/cloud) e i Mediagent presenti presso il Data Center Primario e i Data Center secondari per consentire il backup delle VM e/o dei dati (Database, filesystem AIX, ecc.).

Per tutti i backup sarà effettuata una ulteriore copia secondaria al completamento della copia primaria presso il Data Center secondario.

Trattandosi di un servizio «self-managed» l'utente ha completa autonomia di gestione nella definizione della policy di backup. All'attivazione del servizio al referente tecnico (comunicato in fase di acquisizione del servizio) saranno inviate le credenziali di accesso alla console del servizio. Alla mail del referente tecnico saranno inviate tutte le mail inerenti alle informazioni del servizio.

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-of-place" 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

4.2 Network

Costituisce oggetto della presente fornitura la messa a disposizione delle Interconnessioni e della connettività network del presente Progetto di fattibilità.

I Data Center oggetto di Fornitura prevedono componenti di Data Center Interconnection (DCI) tramite interfacce DWDM, di Virtual Local Area Network prevedendo una portata di Traffico, ruotata nei Data Center cifrata su suolo pubblico.

Il degrado delle caratteristiche trasmissive rispetto ai valori richiesti e sopra riportati o l'interruzione fisica della fibra ottica verranno considerate entrambe come guasto.

La NewCo PSN si farà carico di tutte le attività di progettazione e set up della Connettività, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.
Tutti i servizi elencati nel presente capitolo sono previsti come necessari nelle modalità di erogazione dei servizi infrastrutturali oggetto del presente documento.

4.2.1 Componente Data Center Interconnection

4.2.1.1 *Il Backbone IP/MPLS*

Le due Region saranno collegate da una rete IP su un backbone **proprietario** IP/MPLS (nx100GBE) impiegando solamente apparati router carrier class. La topologia di rete sarà di tipo "Hub and Spoke" in cui gli spoke, i DC, sono collegati in modalità "Dual Homing" agli hub, i POP Centro Servizi. Il "Dual Homing" è reso ancora più affidabile attraverso un POP Centro Servizi fisicamente costruito su due centrali differenti. Gli hub sono collegati fra di loro, almeno nel primo rilascio, secondo una topologia partial mesh. Questa topologia garantirà sulla direttrice che collega le due Region il minimo valore di round trip delay (RTT). Tale backbone consentirà inoltre la configurazione di connettività L2 extension tra ciascun DC.

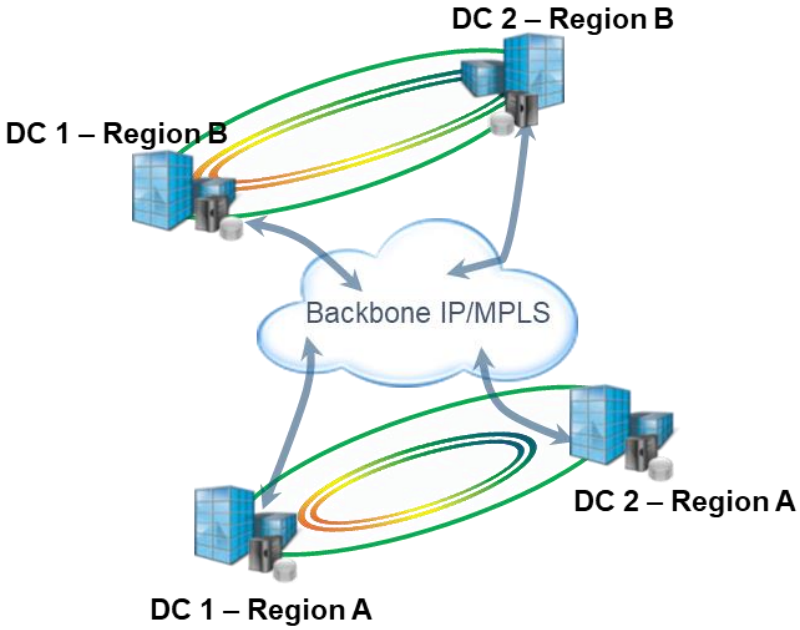


Figura 17: Connessione Data Center

Le interconnessioni tra i due Data Center della stessa Region sono realizzate attraverso percorsi indipendenti garantendo una differenza sulla lunghezza di cavo posato non superiore al 20% rispetto al cavo con lunghezza superiore.

4.2.1.2 *Interfaccia Dense Wavelength Division Multiplexing*

Le componenti di Data Center Interconnection prevedono un'interfaccia Dense Wavelength Division Multiplexing (DWDM) **dedicata con traffico cifrato su suolo pubblico**. I Data Center sono interconnessi tra di loro, allo scopo di realizzare un unico campus, attraverso una coppia di collegamenti metropolitani a 100 GBE dedicati.

4.2.1.3 *Virtual Local Area Network*

Le VLAN sono trasportate in ciascun Data Center e all'interno della stessa Region grazie alla tecnologia VXLAN che estende i limiti delle VLAN, mantenendo la separazione dei contesti di ciascun cliente. I Data Center sono interconnessi attraverso una coppia di collegamenti metropolitani a 100 GBE dedicati.

4.2.1.4 *Traffico*

I Data Center saranno realizzati con delle fabric L3 con topologia spine-leaf. Sia il traffico L2 in tunnelling VXLAN sia il traffico L3 routed è veicolato nativamente all'interno di ciascun campus/DC e viene cifrato su ogni matrice di traffico (potendone anche configurare end to end le singole tratte). Questo modello di interconnessione di fatto consente di avere una completa configurazione di interconnessione full mesh (con encryption) tra tutti i singoli DC costituenti i due differenti campus (region).

4.2.2 Componente Wide Area Network

La componente di Wide Area Network dovrà prevedere la disponibilità della **connessione Internet condivisa con gli altri servizi Data Center su reti condivise e con doppio upsteam provider**:

- Servizio di DDOS Protection condiviso;
- Intrusion Detection System condiviso: possibilità di eseguire servizi di tipo Intrusion Detection per il traffico cliente e ricevere/gestire allarmi tramite SOC
- Annuncio reti internet da entrambi i DC in modalità indifferenziata (Active/Active)

4.2.2.1 *Internet/Infranet Condivisa*

Il backbone IP/MPLS offre connettività Internet e Infranet (SPC Connettività) effettuando peering diretto con il backbone nazionale attraverso tre POP centro Servizi: NORD, Centro NORD e Centro SUD. I POP Centri Servizi sono collocati per questione di affidabilità presso due Centrali Dati e sono ridondati; di conseguenza i punti di peering sono ben sei, ed è impiegata una logica di prossimità geografica che, allo scopo di minimizzare il delay, costringe a due i punti di ingresso/uscita.
Sui GW di peering del backbone nazionale è realizzato l'immediato rilancio verso la QXN (Servizi di Connettività SPC).
La banda condivisa che sarà messa a disposizione delle amministrazioni contraenti è di 10Gb.

4.2.2.2 *Profilatori di Traffico (Bandwindth management)*

In linea agli apparati di DDoS protection, saranno inseriti dei profilatori di traffico. L'obiettivo è quello di realizzare una piattaforma tecnologica dedicata alla profilazione del traffico afferente a e proveniente dai DC interconnessi alla rete di backbone. Il profilatore di traffico offre la possibilità di creare delle Classi di Servizio per ciascun cliente e offre la possibilità di processare i pacchetti transitanti dai segmenti interessati consentendo di poter effettuare una serie di operazioni richieste dal cliente in fase di stesura dei requisiti tra cui:

- Operazioni di Traffic Classification e Traffic Shaping;
- Decision Marking;
- Policy Enforcement.

Il sistema di gestione QoS consente di creare policy gerarchiche multilivello per utente/gruppi di utenti, servizi, encapsulation (GRE, VLAN), Time of day, DSPC applicando azioni di

- Shaping: possibilità di stabilire una banda massima, banda minima garantita, Priorità, garantendo così l'utilizzo massimale della banda e politiche di "fair usage" tra utenti;
- block/alert /bypass;
- expedite forwarding: consente inoltro rapido dei pacchetti per protocolli sensibili a Jitter;
- steering: la piattaforma supporta deviazione/mirror del traffico in tempo reale verso applicazioni di terze parti;
- http redirection.

Gli apparati saranno completamente trasparenti alla rete, non andando a modificare nulla nei pacchetti che transitano sui link attestati. Inoltre, per preservare la connettività anche in caso di guasto, gli apparati sono dotati di un bypass passivo che permetterà in ogni caso il transito del traffico di rete.

Inoltre saranno applicabili meccanismi Deep Packet Inspection (DPI), che consentono il riconoscimento di un elevato numero di applicazioni e la classificazione della maggior parte del traffico presente sulla rete. Il motore DPI contiene una libreria completa di "signatures" per il riconoscimento di ciascun protocollo/applicazione, nonchè la possibilità di creare "signatures" personalizzate. La libreria delle firme viene aggiornata continuativamente tramite i pacchetti di protocollo pack; gli aggiornamenti sono automatizzati.

4.2.2.3 *IDS e APM*

Ciascun Data Center sarà equipaggiato con Network Packet Broker (NPB). Tali apparati permettono di prelevare il traffico tra gli apparati di rete presso il DC (i FW oppure i LB piuttosto che i Router di Edge dedicati) sia in modalità Online sia in Mirroring e quindi di monitorare lo stesso in tempo reale. I NPB, pertanto, sono dotati di porte in "Bypass" attraverso le quali mettono in comunicazione gli apparati di rete e di porte "Tool" attraverso le quali inviano il traffico prelevato agli apparati di monitoraggio siano essi passivi (APM, IDS) o attivi (IPS) dedicati.

4.2.2.4 *Raccolta linee*

I DC messi a disposizione della PA da parte del PSN saranno collegati sia ad Internet sia alla rete SPC, il che consentirà alle Amministrazioni contraenti di ***usufruire dei servizi senza soluzione di continuità.***

4.2.2.5 *Virtual Private Network*

Su base progetto sarà data la possibilità alle PA di realizzare la soluzione VPN ipsec per la crittografia end to end:

- **VPN IPSEC dedicata su infrastruttura dedicata.** Gestione VPN internet con terze parti con la possibilità di gestire piani di indirizzamento in overlap, attraverso la presenza di

terminatori IPSEC fisici o virtuali dedicati in grado di instaurare una VPN IPSEC e di gestire piani di indirizzamento remoti in overlap con quelli in uso.

- **VPN remote access.** Gestione accessi remoti VPN client con terminazione TLS, con la possibilità di gestire e configurare accessi al DC in modalità client e clientless (https) sicura.

4.2.2.6 *Connettività dedicata per la migrazione dati*

Come servizio opzionale, la NewCo PSN offre la possibilità alle PA che ne faranno richiesta, di fruire di connettività dedicata a partire da 1 Gbps su protocollo gigabit ethernet attraverso la quale è possibile realizzare l'accesso alla rete geografica per i servizi necessari alla migrazione dei dati.
I servizi ad alta velocità prevedono l'utilizzo di infrastrutture in fibra dedicata per collegare la sede del cliente con i punti di accesso al servizio gestito dalla NewCo PSN fino al Data Center di destinazione. L'offerta è caratterizzata da:

- elevate prestazioni (sia in termini di picco che di banda garantita);
- affidabilità;
- sicurezza.

Obiettivo fondamentale è quello di proporre un servizio ai massimi livelli di eccellenza in termini di profilo di servizio, di competenza, supporto tecnico e gestione operativa.L'offerta prevede un servizio di Virtual LAN a livello metropolitano tra le sedi del cliente e il DC con velocità di 1Gbps su protocollo Gigabit Ethernet e la realizzazione di una Rete Privata Virtuale "Globale" (VPN IP), in ambito geografico. L'implementazione delle VPN IP utilizza la tecnologia MPLS, basata sull'instradamento dei pacchetti mediante l'inoltro di etichette ad essi associate (Label Swapping). MPLS non utilizza dunque indirizzi IP pubblici, risultando in questo modo inattaccabile dall'esterno e sicura al pari di una rete ATM/FR e flessibile come una rete IP.
Il servizio prevede la fornitura in sede cliente dell'apparato (Terminazione di rete) installato e gestito da personale della NewCo PSN. In caso di connettività richiesta superiore a 1 Gbps, sono previste le bande a 2 Gbps, 5Gbps e 10 Gbps; per queste bande, per le quali sarà necessaria una proposizione a progetto, l'accesso fisico è realizzato su Lambda Wave (fibra ottica DWDM); per tali reti, i parametri di jitter e packet loss sono trascurabili, mentre la latenza varia in base alla lunghezza delle tratte in fibra e al numero di apparati di rete attraversati. In questo caso, la fibra ottica prevista, l'interfaccia di rete e la capacità di inoltro della CPE consentono di effettuare eventuali upgrade di banda rispetto alla scelta iniziale (dunque da 2Gbps fino a 10 Gbps) senza dover apportare modifiche alle configurazioni hardware ma solo attraverso una riconfigurazione logica.

4.2.2.7 *Hosting del router di terminazione*

Nel caso in cui la PA disponesse di un proprio collegamento geografico dedicato (MPLS), è prevista la possibilità di un hosting della terminazione (router) presso i locali DC in prossimità della sala sistemi.
Questo servizio prevede la disponibilità di spazio fisico in un rack adibito allo scopo e con le seguenti caratteristiche:

- Facilities strutturate;
- Cablaggio strutturato in fibra verso la sala TLC;
- Cablaggio in rame verso la DMZ che ospita i gateway dei sistemi Cliente;

- Attività di configurazione della LAN di raccordo tra i gateway Cliente e la terminazione geografica.

La soluzione richiede una verifica propedeutica di posizionamento dell'apparato e utilizzo di bretelle di collegamento.

4.2.3 Componente Local Area Network

I Data Center prevedono la disponibilità dei seguenti apparati in merito alla componente Local Area Network (LAN).

4.2.3.1 *Apparati condivisi (locali in DC o estesi sui due DC)*

Di seguito l'elenco degli apparati dedicati previsti per l'erogazione dei servizi oggetto del presente Progetto di Fattibilità, tutti costantemente monitorati:

- **FIREWALL** segregazione della rete
  - DMZ dedicata su interfacce condivise 1 Gbs: DMZ logica (vlan) dedicata su firewall condiviso con interfacce 1 Gbs;
  - DMZ dedicata su interfacce condivise 10 Gbs: DMZ logica (vlan) dedicata su firewall condiviso con interfacce 10 Gbs.
- **APPLICATION DELIVERY CONTROL:**
  - Servizio di bilanciamento e terminazione sessioni TLS con gestione certificato: virtual server logico dedicato su bilanciatore condiviso con altri servizi/clienti.
  - Web Application Firewall: policy WAF dedicate ed agganciate a virtual server logico, tramite licenza Application Security Manager su bilanciatore condiviso.
  - Autenticazione, SSO, CRL: configurazione Application Policy Manager su virtual server logico dedicato su bilanciatore condiviso.
- **ROUTER**
  - Tabella di routing dedicata su dominio routing condiviso: VRF dedicata su infrastruttura di Data Center condivisa.
- **SWITCH**
  - Broadcast domain dedicato su dominio di switching condiviso: VLAN dedicata su infrastruttura di Data Center condivisa. Gli switch utilizzati e proposti nel ruolo di LEAF per la raccolta della connettività esterna (internet/infranet), verso la farm, piuttosto che gli apparati L4/L7, sono equipaggiati:
  - per la raccolta in fibra con 48 x 1/10/25-Gbps fiber ports (lato host) e 6 x 40/100-Gbps (lato spine);
  - per la raccolta in rame con 48 x 100M/1/10GBASE-T ports (lato host) e 6 x 40/100-Gbps (lato spine);
  - gli switch utilizzati e proposti nel ruolo di SPINE, sono apparati modulari carrier-class equipaggiati con porte 100 GBE.

- **DNS**
  - Gestione entry su dominio dedicato ai servizi della NewCo: setup entry dedicate su zona gestita tramite DNS autoritativi.
- **NAC area uffici e area housing**
  - Gestione di un'area di Office tramite accessi su switch completamente dedicati e separati da quelli di Datacenter. Gli switch di ufficio eseguiranno autenticazione 802.1x colloquiando con un radius (infranet controller) e con autenticazione finale dell'utente in modalità Two Factor demandata ad un server ldap centralizzato. I laptop autorizzati avranno un client installato in grado di colloquiare in 802.1x ed in maniera centralizzata saranno controllate le caratteristiche del client (host checker) che dovrà soddisfare i requisiti minimi di sicurezza (es. allineamento antivirus, etc)
  - Gestione dell'area housing tramite accessi su switch che eseguiranno autenticazione 802.1x colloquiando con un radius (infranet controller). Tale soluzione può essere esclusa se le misure di sicurezza fisica permettono di garantire un adeguato need-to-access alle reti

4.2.3.2 *Apparati dedicati (locali in DC o estesi sui due DC)*

Su base progetto verranno resi disponibili i seguenti apparati:

- **FIREWALL**
  - Firewall L4 interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs.
  - Firewall L4 interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs.
  - Firewall UTM interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs e licenza UTM.
  - Firewall UTM interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs e licenza UTM.
  - Firewall NGFW interfacce 1 Gbs: firewall appliance con interfacce ad 1 Gbs e licenza NGFW.
  - Firewall NGFW interfacce 10 Gbs: firewall appliance con interfacce a 10 Gbs e licenza NGFW.

La gestione unificata degli attacchi, comunemente abbreviata in UTM, è un termine inerente alla sicurezza informatica, che indica una singola soluzione e, una singola applicazione di protezione che offre più funzioni di sicurezza in un unico punto della rete. Un'applicazione UTM include, normalmente, funzioni come: antivirus, anti-spyware, anti-spam, firewall di rete, rilevamento e prevenzione delle intrusioni, filtraggio dei contenuti e protezione dalle perdite di dati. Tutte queste applicazioni (application filtering, IPS, AntiVirus, Web Filtering, Domain Reputation AntiSpam etc), sono disponibili sui dispositivi FW proposti.

- **APPLICATION DELIVERY CONTROL**

- Servizio di bilanciamento e terminazione sessioni TLS con gestione certificato: bilanciatore appliance.
- Web Application Firewall: licenza Application Security Manager su bilanciatore appliance.
- Autenticazione, SSO, CRL: licenza Application Policy Manager su bilanciatore appliance.
-

- **SWITCH**
  - Switch interfacce 1 Gbs: switch con interfacce ad 1 Gbs.
  - Switch interfacce sino 10 Gbs: switch con interfacce sino a 10 Gbs (sfp).
- **DNS**
  - Gestione zona dedicata: gestione della zona del cliente su DNS autoritativi internet.
- **NAC**
  - Gestione dell'accesso dei client autorizzati ad un'area Office.

4.3 Facility

I Servizi di Facility consistono nella messa a disposizione, da parte della NewCo PSN, di aree all'interno dei Data Center, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti:

- Spazi attrezzati;
- Sistemi HVAC;
- Sicurezza Fisica;
- Rack e Cage.

Il dettaglio dei servizi è descritto nel ***capitolo 5 – Caratteristiche Data Center***.
La NewCo PSN si farà carico di tutte le attività di progettazione e set up delle Facilities, propedeutico all'erogazione dei Servizi descritti nel presente capitolo.

4.3.1 Energia Elettrica

Il Servizio prevede la Fornitura dell'energia elettrica necessaria all'alimentazione delle infrastrutture descritte nel presente Progetto di fattibilità.

La NewCo PSN fornirà ad ogni PA con cadenza mensile, un report afferente i consumi elettrici relativi alle infrastrutture oggetto del Servizio, riportante:

- La potenza elettrica complessivamente assorbita nel mese precedente (espressa in kW) relativa a ciascun rack e derivante dall'insieme di apparati IT e TLC presenti

- La potenza elettrica complessivamente assorbita nel mese precedente (carico IT, espressa in kW) quale sommatoria delle potenze elettriche assorbite dalla totalità dei rack (kWIT)

Il prezzo dell'energia elettrica è composto da alcune componenti variabili nel tempo e non controllabili dalla NewCo PSN, quali:

- PUNIndex: è la media aritmetica mensile, espressa in Euro/kWh e arrotondata alla seconda cifra decimale, dei valori orari del PUN (), rilevati sulla piattaforma telematica: Mercato Elettrico – Mercato Elettrico a pronti (MPE) – Mercato del Giorno Prima (MGP). Tale quotazione, al momento di pubblicazione del presente bando, risulta pubblicata sul sito internet del GME tra i dati di sintesi MPE-MGP – riepilogo; colonna media dei Prezzi d'acquisto, PUNIndex (€/kWh) della sintesi mensile, nella sezione Esiti dei mercati e statistiche – Statistiche;
- Oneri: oneri di sistema del solo Mercato Libero (a titolo esemplificativo le componenti tariffarie A, UC, MCT), come stabiliti, volta per volta, dall'AEEGSI (www.autorita.energia.it). Relativamente algi oneri verrà riconosciuta alla NewCo PSN esclusivamente delle tariffe la parte variabile (solo la quota addebitabile al cliente finale espressa in €/kWh)
- Dispacciamento: corrispettivi relativi alle componenti che costituiscono i costi per il dispacciamento sul mercato libero (le cui componenti sono pubblicate da TERNA e dall'AEEGSI);
- Perdite di Rete: prezzi unitari dovuti per le perdite di energia elettrica dati dal prodotto dei fattori percentuali di perdita di energia elettrica sulle reti con l'obbligo di connessione di terzi così come definite nella colonna (A) della Tabella 4 del TIS e delle voci "PUNIndex" e "Dispacciamento" precedentemente definite;
- Trasporto: oneri di Trasmissione, Distribuzione e Misura, così come stabiliti, volta per volta, dall'AEEGSI. Relativamente al trasporto verrà riconosciuta alla NewCo PSN esclusivamente delle tariffe la parte variabile (solo la quota addebitabile al cliente finale espressa in €/kWh)
- Fiscalità: tassazione prevista dalla normativa vigente relativa alla fornitura di energia elettrica al netto della sola IVA.

Essendo le componenti sopra descritte variabili nel tempo e non controllabili dalla NewCo PSN, sarà previsto durante l'esecuzione del contratto un meccanismo di aggiornamento delle tariffe esposte, con cadenza trimestrale su base mensile.

5 Caratteristiche Data Center

I siti saranno localizzati in un'area servita da connettività SPC, i cui tre fornitori di riferimento sono stati selezionati nell'ambito della Gare per l'affidamento dei servizi di connettività (ID Sigef 1367), la cui composizione è stata pubblicata il 15/06/2016 sul sito dell'Agenzia per l'Italia Digitale.

Saranno rispettate tutte le disposizioni attualmente vigenti relative alle infrastrutture di Information Technology, quali:

- Requisiti indicati dal D.Lgs. 81/2008 Testo Unico sulla salute e sicurezza sul lavoro;
- Cavi UTP rispondenti a ISO/IEC 11801 almeno categoria 5;

5.1 Determinazione caratteristiche del macrosistema Data Center

Caratteristiche dei Data Center

La NewCo PSN prevede di impiegare **n.4 Data Center** aventi caratteristiche aderenti allo **standard ANSI/TIA 942**, coerentemente con quanto indicato da AgID nelle "*Linee guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione*", pubblicate sul sito dell'Agenzia (https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lg_razionalizzazione_ced_pa_0.pdf)

aventi le specifiche di seguito riportate:

- I 4 Data Center saranno allestiti in doppia Region (2 DC + 2 DC), la singola Region avrà i due diversi Data Center distanti almeno 5 Km in linea d'aria e non più di 60 Km di distanza in fibra in doppio percorso completamente distinto fra l'uno e l'altro, evitando così di avere un singole point of failure (SPOF); posizionati ad una distanza adeguata all'erogazione di servizi Active-Active Geografico. La latenza garantita è definita nei capitoli relativi alle caratteristiche di connessione;
- Le due Region saranno geograficamente posizionate ad una distanza tale da consentire la realizzazione di tutti i servizi di Disaster Recovery in maniera efficace. Nello specifico esse saranno ubicate ad una distanza **minima di 500 Km** all'interno del territorio nazionale in aree con condizioni di rischio diverse tra loro. Nelle valutazioni di rischio considerate si citano, a titolo indicativo ma non esaustivo:
    - Rischio sismico;
    - Rischio idrogeologico;
    - Rischio ambientale;
    - Rischio terroristico;
    - Rischio inquinamento ambientale e/o industriale
- La soluzione proposta prevede di utilizzare in una prima fase 2 Data Center con le seguenti caratteristiche:
    - un Data Center di una delle due Region in possesso delle seguenti certificazioni:

- **UPTIME INSTITUTE Tier IV Constructed Facilities;**
- **ANSI TIA 942 Rating 4**;
- EN 50600 classe 4;
- ISO 27001;
- ISO 14001.

  - un Data Center di una delle due Region in possesso delle seguenti certificazioni:
    - **UPTIME INSTITUTE Tier IV Design Facilities;**
    - entro 3 mesi dalla sottoscrizione della convenzione certificazione **UPTIME INSTITUTE Tier IV Constructed Facilities;**
  - I 2 ulteriori Data Center in possesso della certificazione **Uptime Institute Tier III Design Facilities e ANSI TIA 942 Rating 3**.

- In una seconda fase si avrà:
  - Entro 21 mesi dalla sottoscrizione della Convenzione, 2 DC certificati **UPTIME INSTITUTE Tier IV Constructed Facilities**;

La configurazione finale prevede l'utilizzo di 4 DC, su due region, tutti certificati sia UPTIME INSTITUTE Tier IV Constructed Facilities sia ANSI/TIA 942 Rating 4.

- Entro 18 mesi dalla sottoscrizione della Convenzione, la NewCo PSN avrà almeno una Region in possesso della certificazione **LEED Gold (cfr. §.5.2.3.1)**.
- Per ognuno dei 4 DC coinvolti nel progetto saranno dedicati gli spazi utili per alloggiare i rack secondo un modello di incremento modulare nel tempo, in funzione delle adesioni delle PA al PSN. Tale crescita parte da uno spazio iniziale di 800mq con potenza complessiva di 1.150 Kw e può incrementare in maniera modulare fino ad uno spazio complessivo di 2.900mq con una potenza totale di 4.800Kw.

Caratteristiche della rete dei Data Center e delle Region:
La topologia di rete di scelta per realizzare ciascun Data Center sarà basata su una architettura Spine-Leaf a 100GBE che utilizza la tecnologia VXLAN per incapsulare i frame layer 2 dentro UDP header con l'obiettivo di estendere il dominio di switching attraverso una rete layer 3 IP. La diffusione delle Informazioni layer 2 (MAC address) e layer 3 (host IP address), affidata al control plane MP-BGP EVPN, rende estremamente scalabile la rete. Una fabric L3 IP inoltre è, per definizione, spanning tree free rendendo la rete più stabile; ha tempi di convergenza molto contenuti (dell'ordine delle decine di msec) e consente in modo semplice ed automatico la distribuzione del traffico tra i vari link e, pertanto, l'utilizzo ottimale delle risorse di rete. IL consumo delle vlan_id è poi ampiamente superato in quanto il VXLAN estende il range delle vlans da 4096 ad oltre 16 milioni. Un altro importante vantaggio di una fabric L3 è la possibilità di attivare il Distributed Gateway che, presentando lo stesso ip address gateway su tutti gli Edge Switch (LEAF), offre ad ogni endpoint la possibilità di essere ruotato localmente nel punto più vicino. Tutti i nodi della fabric sono dual stack, caratteristica fondamentale per introdurre il protocollo ipv6 senza dover ricorrere a tecniche di tunnelling o di NAT che limitano inevitabilmente la scalabilità della rete. Le fabric Spine-Leaf di ciascun Data Center dell'architettura richiesta dovranno esser unite tra di loro attraverso dei collegamenti metropolitani a 100 GBE dedicati. Tuttavia, per superare i limiti di scalabilità delle stretched

fabric, sono impiegati dei nodi L3, che da un lato sono collegati agli spine locali e d'altro terminano i collegamenti di DCI metropolitani con la controparte dell'altro Data Center. La topologia di rete che risulta si chiama Multi POD.

I Data Center utilizzati adotteranno la tecnologia SDN (software defined networking) per il controllo centralizzato e automatizzato di tutti i processi, dal deploy di una nuova applicazione alla relativa manutenzione e monitoraggio. In particolare, **i due Data Center di ciascuna Region saranno gestiti da un unico controller SDN** che, per ragioni di alta affidabilità, sarà costituito da un cluster di server distribuiti tra le due fabric. La Region può essere pertanto considerata come un unico campus, caratterizzato da un unico dominio VXLAN che rende l'estensione L2 tra i due Data Center come qualcosa di intrinsecamente sempre valido e garantito senza dover intervenire in alcun modo sui collegamenti che realizzano il DC Interconnection. Sfruttando il controller SDN, si realizzerà una architettura multisite tra le due Region, realizzando un vero e proprio Campus geografico, non solo per estendere e mettere a fattor comune risorse tra le due Region ma anche per scopi di disaster recovery.

5.1.1 Caratteristiche geografiche e topografiche

I Data Center saranno posizionati in aree di rischio sismico classificate come zona non inferiore alla zona 3 secondo il DM 58 del 2017. Per quanto attiene al rischio idrogeologico, le strutture sono presenti in aree a basso rischio. Nel caso in cui l'area presenti potenziali rischi, sarà data evidenza di tutte le azioni correttive adottate al fine di gestire e superare le eventuali criticità.

Dal punto di vista dei rischi ambientali ed esterni si manifesta la preferenza per siti aventi le seguenti caratteristiche intrinseche:

- Lontananza significativa da vie costiere o vie navigabili interne;
- Lontananza dalle principali arterie di traffico;
- Vicinanza alle grandi aree metropolitane;
- Distanza inferiore o uguale a 10 km e uguale o non superiore a 50 km rispetto ad aeroporti.

5.1.2 Indipendenza connessioni elettriche ed impiantistiche

Le infrastrutture tecnologiche dei Data Center non avranno punti di alimentazione esterna comune.

Al fine di meglio chiarire l'affermazione, non sono utilizzati Data Center alimentati dalla medesima sottostazione di alta tensione e/o derivati dalla stessa rete urbana di media tensione.

5.2 Determinazione caratteristiche dei singoli Data Center

5.2.1 Caratteristiche dimensionali del sito

Di seguito si riportano le caratteristiche dimensionali target che saranno rese disponibili per ogni sito:

- Spazio netto data-room disponibile: ognuno dei 4 DC coinvolti nel progetto metterà a disposizione gli spazi dedicati utili per alloggiare i rack secondo un modello di incremento modulare nel tempo, in funzione delle adesioni delle PA al PSN. Tale crescita parte da uno spazio iniziale che varia da 100 mq a 350 mq e può incrementare in maniera modulare fino ad uno spazio complessivo che varia da 250 mq a 700 mq.
- Potenza IT disponibile: non inferiore a 1.150 KW totale al tempo T0.
- Numero rack da ospitare: non inferiore a 100 complessivi al tempo T0, riproporzionati sulla base dei mq dei singoli siti.

5.2.2 Caratteristiche topografiche ed ambientali

La configurazione topografica del datacenter, oltre alle sale informatiche ad uso esclusivo richieste al punto precedente, garantirà anche la presenza dei seguenti spazi e/o servizi accessori:

- Magazzino a temperatura controllata con spazio segregato dedicato non inferiore ai 50 mq;
- Disponibilità di "TEST AREA" ad uso condiviso per la prova e test delle apparecchiature informatiche prima dell'installazione in dataroom;
- Aree condivise di smart working per tecnici e specialisti;
- Baia di carico/scarico merci, con percorso dedicato ed indipendente dal percorso pedonale. Tale area sarà monitorata e controllata dal sistema di vigilanza.

5.2.3 Caratteristiche architettoniche e strutturali

Di seguito si riportano le caratteristiche architetturali e strutturali target che saranno rese disponibili per ogni sito:

- Portata pavimenti non inferiore a 800 kg/mq
- RACK da 42, 48, 52
- Vie di accesso garantite alle dataroom non inferiori a 1200 x 2100 mm netti;

5.2.3.1 *Sostenibilità energetica e certificazioni*

I Data Center sono gestiti nel segno dell'efficienza energetica e della sostenibilità ambientale; la NewCo PSN adotta politiche e modelli produttivi che riducono al minimo le emissioni e limitano l'utilizzo delle risorse ambientali.

La NewCo si doterà di edifici costruiti e gestiti secondo principi "green", ovvero prevedendo le più avanzate tecniche di raffreddamento, ma anche soffitti e mura in grado di gestire al meglio la temperatura, l'impiego di batterie agli ioni di litio al posto di quelle al piombo, di luci LED a basso consumo energetico, impianti fotovoltaici che contribuiscono al contenimento del PUE.

Vengono utilizzati dispersori geotermici ad una profondità di 30 mt per lo smaltimento del calore prodotto dai Gruppi Frigo, raddoppiando così il rendimento degli stessi.
In alcuni Data Center si utilizzano D-UPS (UPS dinamici) che non hanno bisogno dell'utilizzo delle batterie andando così ad aumentare la sostenibilità ambientale.
Gli apparati più datati, che richiedono un maggiore consumo di energia, vengono costantemente sostituiti con apparati nuovi e in grado di beneficiare di soluzioni più efficienti, come l'EPV (Evaporative Free Cooling), che permettono di ridurre i costi e di garantire una maggiore resilienza operativa.

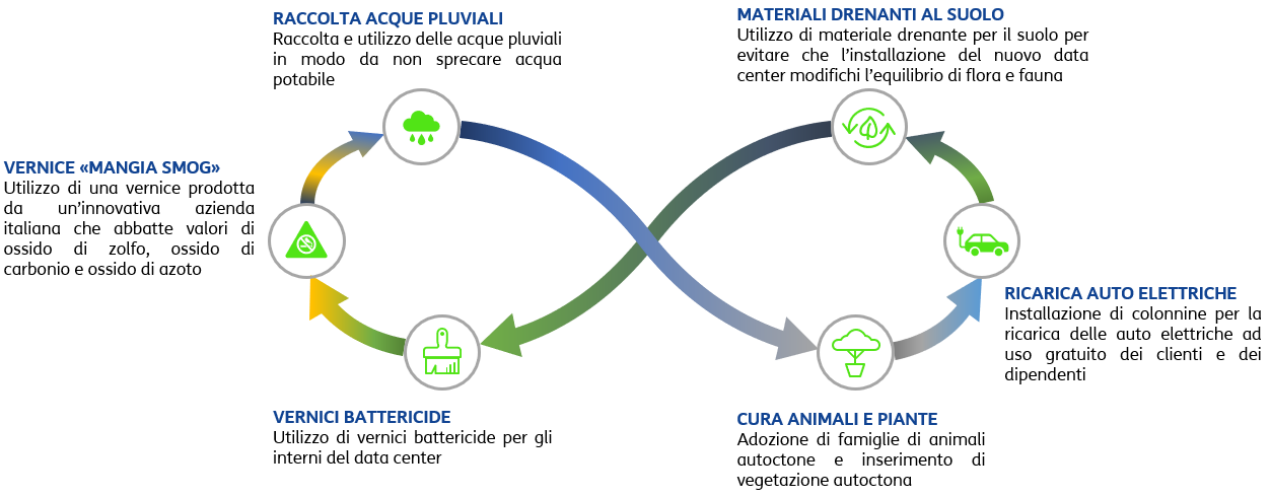


Figura 18: Ciclo virtuoso energia dei Data Center

Per quanto riguarda il footprint ambientale, i DC hanno fissato l'obiettivo di raggiungere il livello di PUE inferiore 1,4 e diventare carbon neutral entro il 2030.

I Data center della NewCo PSN potranno inoltre vantare le seguenti certificazioni:

Certificazione ISO 50001
Per le aree che hanno un impatto rilevante sulla Comunità, attraverso prodotti e servizi offerti, i Data Center impiegati dall NewCo PSN hanno ottenuto le certificazioni che assicurano l'adozione di procedure e comportamenti in linea con le aspettative degli stakeholder. In particolare, la norma ISO 50001 è la certificazione relativa a requisiti per creare, avviare, mantenere e migliorare un sistema di gestione dell'energia ed ottimizzare in modo continuo la propria prestazione energetica.
La norma definisce i requisiti applicabili all'uso e consumo dell'energia, includendo l'attività di:

- misurazione,
- documentazione,
- progettazione,
- acquisto per le attrezzature,

nonché i processi e il personale che contribuiscono a determinare la prestazione energetica.

Certificazione ISO 14001
I Data Center impiegati dalla NewCo PSN possono vantare la certificazione ISO 14001 che è la norma di riferimento per le aziende dotate di un Sistema di Gestione Ambientale. I requisiti

prevedono che il "Sistema di gestione Ambientale" sia parte integrante del sistema di gestione aziendale e sia volto a gestire gli aspetti ambientali, soddisfare gli obblighi di conformità legislativa e affrontare e valutare i rischi e le opportunità.

Certificazione LEED

La certificazione costituisce una verifica di parte terza, indipendente, delle performance dell'intero edificio sede del Data Center. La certificazione LEED, riconosciuta a livello internazionale, afferma che un edificio è rispettoso dell'ambiente e che costituisce un luogo salubre in cui vivere e lavorare. L'ottenimento della certificazione LEED permette di ottenere sia vantaggi economici che ambientali, tra cui:

- stabilire uno standard comune di misurazione dei "green buildings", definiti come edifici a basso impatto ambientale;
- fornire e promuovere un sistema di integrato di progettazione che riguarda l'intero edificio;
- la riduzione dei rifiuti inviati in discarica, esempio di economia circolare;
- i risparmi energetico e idrico, utilizzando free-cooling e la gestione delle acque meteoriche;
- lo sviluppo di edifici più sani e più sicuri, abolendo il fumo e garantendo la qualità dell'aria;
- la creazione di comunità compatte e accessibili, con buon accesso ai servizi di vicinato e di transito;
- la tutela delle risorse naturali, incoraggiando lo sviluppo urbano in zone già antropizzate;
- la riduzione delle emissioni nocive di gas serra, utilizzando gas non nocivi.

5.2.4 Infrastruttura elettrica

5.2.4.1 *Impianto di terra e protezione scariche atmosferiche*

L'intero insediamento sarà attrezzato con un impianto di terra adeguatamente dimensionato e realizzato in accordo alle norme vigenti.
All'impianto di terra faranno capo:

- Impianto di protezione elettrica;
- Impianto di equalizzazione del potenziale realizzato all'interno dell'insediamento e nelle dataroom a servizio degli armadi racks;
- Impianto di terra "pulita" informatica necessaria ad alcuni apparati IT;
- Impianto di protezione scariche atmosferiche.

L'intero Data Center sarà protetto da impianto di protezione dalle scariche atmosferiche. Saranno altresì protetti da impianto di captazione tutti i manufatti e le apparecchiature inerenti al Data Center posizionati all'esterno.

5.2.4.2 *Stazione di energia normale*

Per i siti certificati Rating 4 e TIER IV l'insediamento sarà alimentato da non meno di due cabine elettriche di trasformazione tra loro indipendenti e segregate da compartimenti antincendio REI120. Ogni cabina apparterrà ad un ramo di alimentazione del Data Center e sarà dimensionata e certificata per garantire l'alimentazione di tutto l'insediamento in caso di down del secondo ramo (configurazione 2N).

5.2.4.3 *Stazione gruppi elettrogeni di emergenza*

L'alimentazione del Data Center sarà garantita in caso di down dell'ente erogatore da stazioni di energia in configurazione minima N+1. I gruppi elettrogeni potranno essere in bassa o media tensione in funzione delle potenze nominali in gioco.

Le macchine saranno dotate di serbatoio combustibile giornaliero a bordo macchina e serbatoio di stoccaggio. Il sistema garantirà una autonomia di funzionamento alla potenza nominale senza rabbocco di carburante non inferiore a 48 ore nelle condizioni di perdita di una sorgente di emergenza per qualsiasi causa o guasto.

5.2.4.4 *Stazione UPS di continuità servizio*

La continuità elettrica sarà garantita da non meno di 2 isole di continuità assoluta (una per ogni ramo di alimentazione) e saranno utilizzate per l'alimentazione del carico IT in configurazione 2N.

Sarà garantita una autonomia minima di 20 minuti a carico nominale certificato con batterie stazionarie alle condizioni di fine vita.

In caso di utilizzo di gruppi statici di continuità di tipo dinamico l'inerzia meccanica dovrà garantire l'alimentazione del carico nominale per non meno di 40 secondi.
I gruppi di continuità saranno alloggiati in locali dedicati e compartimentati rispetto agli altri locali tecnici.

Le batterie saranno installate in locali tecnici ad esse dedicati, compartimentati tra loro e verso gli altri locali. Saranno inoltre dotati di sistema di ventilazione forzata e sensori di rilevazione della presenza di idrogeno. Le batterie dei gruppi di continuità saranno monitorate da un impianto di controllo e verifica dello stato delle batterie per analizzare lo stato di esercizio delle stesse nelle condizioni ordinarie di funzionamento ed in condizioni di scarica e ricarica.

5.2.4.5 *Sistema pulsanti di sgancio di emergenza*

Il Data Center sarà dotato di un impianto di sganci di emergenza realizzato in accordo con le richieste di prevenzione incendi. Gli impianti dovranno comunque rispettare le seguenti precauzioni minime:

- Sarà realizzato un quadro di sgancio di emergenza per ogni ramo di distribuzione elettrica. I quadri saranno installati in locali differenti e compartimentati tra loro. I cavi saranno posati in canalizzazioni dedicate ed identificate solo per tale scopo e viaggeranno in compartimentazioni antincendio separate.
- Dovranno essere predisposti pulsanti di sgancio differenti per i vari servizio:

- Sgancio energia normale;
- Sgancio sorgenti di emergenza (possibilmente con sganci singoli per ogni gruppo elettrogeno);
    - Sgancio sorgenti in continuità assoluta (uno sgancio per ogni isola e/o per ogni gruppo di continuità assoluta).

5.2.4.6 *Rete di distribuzione primaria e secondaria*

La distribuzione elettrica primaria e secondaria sarà realizzata mediante distribuzione in cavo su passerelle e/o con l'utilizzo di condotti sbarra prefabbricati.

All'interno delle sale informatiche, così come nelle altre aree del Data Center, la distribuzione primaria (dalle cabine elettriche ai quadri di zona) e la distribuzione secondaria (dai quadri di zona alle utenze finali) dovranno essere realizzate con canalizzazioni separate ed adeguatamente identificate.

Dovranno inoltre essere garantite le separazioni delle vie cavi relative a servizi diversi. Per tale motivo saranno opportunamente predisposti canalizzazioni differenti per servizi di distribuzione elettrica, impianti ausiliari, impianti di trasmissione dati primaria e secondaria; distribuzione dati in fibra ottica ed in rame ed impianti di sicurezza.

5.2.4.7 *Impianti di illuminazione*

All'interno di tutte le aree del Data Center (sale informatiche e spazi tecnologici) sarà realizzato un impianto di illuminazione atto a garantire l'adeguato livello di illuminazione previsto dalle normative vigenti nelle sale informatiche e nelle aree tecnologiche.

All'interno di ogni locale sarà garantita la presenza dell'illuminazione da sorgenti in continuità assoluta e da sorgente di emergenza (interruzione breve).

Sarà inoltre realizzato un impianto di illuminazione di sicurezza con apparecchi muniti di gruppo autonomo di emergenza (autonomina minima garantita 60 minuti) o con soccorritore centralizzato. Tale impianto garantirà un livello minimo di illuminazione di sicurezza non inferiore ai 5 lux.

5.2.4.8 *Impianti di forza motrice dataroom*

L'infrastruttura elettrica del Data Center garantirà l'alimentazione standard per ogni rack costituita da:

- Presa industriale interbloccata 230V – 32 A - alimentazione di ramo A;
- Presa industriale interbloccata 230V – 32 A - alimentazione di ramo B.

Le singole linee elettriche saranno protette singolarmente da interruttore automatico dedicato. Ogni linea sarà opportunamente monitorata al fine di verificare e controllare gli assorbimenti elettrici ed i consumi energetici. Gli assorbimenti elettrici sono misurati per singolo blindo ovvero per singola fila di rack.

5.2.4.9 *Rete infrastruttura per manutenzione*

Come indicato nelle pagine precedenti la proposta è atta a garantire una infrastruttura elettrica avente caratteristiche tecniche coerenti con il rating TIER III/3 Uptime Institute o ANSI TIA.

Le infrastrutture, coerenti ai requisiti imposti dagli enti sopracitati, prevedono la possibilità/ di effettuare la corretta manutenzione degli apparati e infrastrutture elettriche garantendo l'alimentazione elettrica in continuità assoluta dei quadri di sala (anche dalla stessa sorgente in continuità assoluta) in caso di spegnimento parziale o totale di un ramo di alimentazione e distribuzione o delle apparecchiature elettriche ad esso collegate.

5.2.5 Infrastruttura climatizzazione

L'impianto di climatizzazione a servizio del Data Center sarà realizzato al fine di traguardare gli obiettivi del rating TIER III/3 minimi riferiti alle normative di certificazione. L'infrastruttura garantirà infatti la possibilità di eseguire qualsivoglia intervento di manutenzione ordinaria o straordinaria garantendo la continuità di esercizio dell'impianto.

All'interno delle dataroom saranno sempre garantite nei corridoi freddi (corridoi in cui è immessa l'aria di raffreddamento) il mantenimento dei valori termoigrometrici all'interno dei range raccomandati da ASHRAE Thermal Guidelines for Data Processing Environments: 18÷27°C, 20÷80% H.R.Il controllo delle condizioni sopra descritte sarà garantito da sonde di temperatura ed umidità connesse al sistema BMS di monitoraggio. Le sonde saranno installate a circa 1,6 m da quota pavimento e dovranno essere in numero congruo a garantire il monitoraggio completo delle sale.

La climatizzazione dei locali tecnici a servizio del Data Center (cabine elettriche, locali UPS, etc.) sarà garantita da impianti in configurazione 2N. Le temperature di esercizio saranno conformi alle caratteristiche delle apparecchiature installate.
I locali contenenti batterie di accumulatori saranno dotati di sistema di estrazione e ricambio d'aria dedicato avente le caratteristiche conformi all'utilizzo in atmosfere con presenza potenziale di idrogeno.

5.2.5.1 *Stazione di energia termica e frigorifera*

Il Data Center avrà sistemi di produzione di energia frigorifera indipendenti al fine di garantire una configurazione minima N+1.

Ogni sistema sarà dimensionato al fine di garantire il corretto raffreddamento dei carichi di progetto nelle condizioni climatiche più estreme relative al luogo di installazione. Per tale verifica saranno considerati le condizioni climatiche previste dall'ASHRAE HANDBOOK a n=20 anni.

5.2.5.2 *Efficienza Sistema di raffreddamento*

Il sistema di raffreddamento del Data Center ed in particolare delle dataroom sarà realizzato al fine di garantire nelle diverse condizioni di carico IT un'efficacia energetica coerente con un PUE massimo di 1.6. Tale valore dovrà essere calcolato considerando tutti i carichi elettrici a servizio

del Data Center, ivi compresi i carichi luce e forza motrice dei locali e/o spazi di servizio da esso collegati.

5.2.5.3 *Sistema di controllo HVAC*

L'impianto di climatizzazione sarà gestito, controllato e comandato da un impianto di termoregolazione a cui faranno capo anche tutti le sonde posizionate nelle dataroom.

5.2.5.4 *Reti di distribuzione idroniche e / o areauliche*

Le reti di distribuzione provenienti dalle due stazioni di produzione indipendenti saranno tra loro separate e compartimentate ai fini antincendio fino all'ingresso della singola dataroom.
Particolare attenzione sarà posta al fine di evitare la possibilità di ghiacciamento dei fluidi all'interno delle tubazioni e delle apparecchiature in caso di installazioni all'esterno in climi particolarmente rigidi nel periodo invernale.

5.2.5.5 *Rete di adduzione*

In caso di utilizzo di impianti di raffreddamento ad acqua di torre, ovvero impianti con utilizzo di acqua di falda e quindi dipendenza dell'infrastruttura di climatizzazione da sorgenti esterne, sarà garantita la presenza di vasche di accumulo adeguatamente dimensionate al fine di garantire una autonomia nel caso di funzionamento in isola dei sistemi di almeno 12 ore nelle condizioni più estreme.

5.2.5.6 *Rete di scarico acque nere ed acque bianche*

Le reti di scarico del Data Center saranno opportunamente allacciate alle reti municipali al fine di evitare qualsivoglia reflusso in caso di eventi straordinari che impattino sulle reti di smaltimento delle acque meteoriche e reflue.

Nel caso questo rischio sia evidenziato, saranno predisposte e proceduralizzate soluzioni tecniche di emergenza da attivare in casi critici.

5.2.6 Impianti ausiliari e protezione incendio

Il Data Center sarà dotato di impianti ausiliari ad alto contenuto tecnologico necessario per la corretta gestione delle infrastrutture, nonché alla riduzione dei rischi di incendio sia per le persone che per le apparecchiature ed i servizi ad esse collegati.

5.2.6.1 *Impianto rivelazione fumi ed antiallagamento*

Tutte le aree del Data Center saranno dotate dei seguenti impianti di rivelazione fumi:

- Impianto VESDA (Very Early Smoke Detection Apparatus). Installato in tutti i locali garantirà una rilevazione precoce di fumo. Non necessariamente entra nelle logiche di comando ed attivazione dei sistemi di spegnimento automatico. È interfacciato con la centrale di rilevazione fumi e/o con il sistema di BMS;
- Impianto rilevazione fumi indirizzato. Installato in tutti i locali secondo le indicazioni della norma UNI9795. Gestisce l'allarme incendio ed è interfacciato con i sistemi di spegnimento

automatico. È caratterizzato da sensori di fumo o calore, pulsanti ad attivazione manuale e segnalatori ottici acustici. Comanda anche tutte le serrande tagliafuoco installate sui canali di ventilazione.

5.2.6.2 *Impianto di diffusione sonora ai fini evacuazione*

Un impianto di evacuazione sarà installato in tutte le aree interne ed esterne e correttamente dimensionato anche in riferimento all'alto rumore di fondo generalmente presente nelle dataroom. Tale impianto sarà interfacciato con il sistema di rilevazione fumo, ma avrà anche la possibilità di comando manuale attraverso una postazione generalmente presente nella security room.

5.2.6.3 *Impianto di supervisione BEMS*

Il monitoraggio e controllo di tutta l'infrastruttura tecnologica sarà garantito dai sistemi BEMS (Building Electrical Management System). I sistemi dovranno essere attivi e funzionanti H24 sempre e comunque. L'architettura informatica hardware e software permette la fruibilità e l'utilizzo delle piattaforme anche in caso di guasto di un elemento costituente l'infrastruttura stessa.

Sulla piattaforma saranno catalogati e memorizzati tutti gli allarmi, le anomalie e le condizioni di funzionamento delle diverse apparecchiature, con la possibilità di visualizzare e storicizzare trend di temperature, umidità, assorbimenti elettrici o altre grandezze ritenute sensibili per la corretta gestione del Data Center.

Il sistema inoltre sarà in grado di trasmettere warning ed allarmi mediante email, sms o altre tecnologie ritenute adeguate allo scopo.

5.2.6.4 *Impianto di estinzione incendio*

Tutte le aree critiche del Data Center saranno protette da impianti di spegnimento incendio automatico. Gli impianti saranno adeguatamente dimensionati e realizzati in riferimento alle condizioni di rischio, ai locali da proteggere ed alle logiche di attivazione.

I Dc saranno dotati di impianti di spegnimento a gas (con l'utilizzo di gas di ultima generazione conformi al protocollo di Kyoto) in luogo di impianti di spegnimento ad acqua.

5.2.6.5 *Sistema di deposito gasolio*

I sistemi di stoccaggio gasolio sono opportunamente progettati in accordo con le regole tecniche di prevenzione incendi ed i decreti ministeriali ad esse associate.

Le stazioni di emergenza avranno serbatoi di stoccaggio indipendenti e possibilmente posizionati in aree diverse all'interno dell'insediamento.

Il sistema di stoccaggio potrà essere costituito da uno o più serbatoi per ogni stazione di emergenza e garantirà l'alimentazione della sorgente per un tempo non inferiore alle 48 ore in caso di alimentazione di tutto il carico elettrico del Data Center.

Il collegamento tra il sistema di stoccaggio gasolio e la stazione di emergenza sarà realizzato da tubazioni opportunamente protette dalla possibilità di congelamento del gasolio. Sarà inoltre presente un sistema di rilevamento perdite gasolio interfacciato coi i sistemi di monitoraggio dell'insediamento.

Ogni sistema di pompaggio del combustibile sarà realizzato con almeno una configurazione N+1 delle pompe elettriche + la presenza obbligatoria di una pompa ad azionamento manuale.

5.2.7 Impianti security

La sicurezza fisica fa parte dell'infrastruttura fisica del Data Center perché ricopre un ruolo fondamentale per ottimizzarne la disponibilità ("uptime"). In tal modo, è possibile ridurre i tempi di fermo dovuti a incidenti o sabotaggi causati dalla presenza di persone inutili o dannose.

Il Data Center avrà un piano di sicurezza semplice: la mappa dell'infrastruttura fisica identificherà le zone e i varchi di accesso che richiedono diverse regole di accesso o livelli di sicurezza.

I confini di queste zone dovranno essere preferibilmente concentrici:

- Perimetro della sede;
- Perimetro dell'edificio;
- Zona computer;
- Sale computer;
- Rack con le apparecchiature.

All'ingresso al sito sarà opportunamente predisposta una postazione di guardiania per l'esecuzione di accurati controlli a vista, ovvero analisi anche con sistemi avanzati per l'individuazione di materiale e/o sostanze pericolose all'interno di zaini, borse o altro (per le persone) e imballi (per il materiale).

5.2.7.1 *Impianto controllo accessi*

L'impianto controllo accessi garantirà l'accesso a tutte le aree del Data Center con le seguenti modalità:

- Spazi non sensibili:
  - Accesso e uscita con badge + pin o sistemi equivalenti (2 livelli di controllo);
- Datarooms:
  - Accesso e uscita con antipass back ed anti accodamento con badge + pin o sistemi equivalenti (2 livelli di controllo);
- Locali tecnici:
  - Il controllo accessi alle sedi deve avvenire almeno tramite lettore di badge;

- Il controllo accessi alle aree critiche deve avvenire con letture di badge + biometrico/pin ovvero con doppio livello di controllo.

Il sistema di controllo accessi sarà gestito dalla security e registrerà tutti gli accessi ed i transiti per almeno 60 giorni.

5.2.7.2 *Impianto antintrusione*

Il sito sarà equipaggiato con un sistema antintrusione ad attivazione automatica interconnesso con sistemi di vigilanza pubblica e/o privata.

L'impianto sarà caratterizzato da sensoristica di protezione perimetrale esterna all'insediamento, sensori di protezione sulle aree di accesso all'edificio, sensori di protezione sui varchi di accesso delle aree interne critiche e sensibili. Alcune aree saranno allarmate H24, altre saranno allarmate in alcune fasce orarie. Sarà possibile escludere le zone in modo selettivo al fine di garantire accessi al personale e/o a clienti e fornitori. L'esclusione della protezione potrà essere eseguita solo dal personale della security mediante opportuni codici univoci. Le esclusioni saranno tracciate e comunicate ai sistemi di vigilanza al fine di garantire almeno un doppio livello di controllo.

Il personale di vigilanza sarà presente in sito H24 con almeno 2 persone. È prevista una ronda programmata con sistema di verifica e conferma installato nelle varie aree del sito.

5.2.7.3 *Impianto di videosorveglianza a circuito chiuso*

Tutto il sito sarà protetto da impianto di videosorveglianza e videoregistrazione. La registrazione delle immagini dovrà garantire uno storico non inferiore a 15 giorni per tutte le telecamere installate. L'accesso al sistema è garantito solo ed esclusivamente al personale di sicurezza adeguatamente identificato dalle procedure e normative in termini di privacy.

L'impianto dovrà garantire:

- Protezione totale perimetrica esterna dell'insediamento;
- Protezione di tutte le aree di accesso all'edificio;
- Protezione di tutte le porte di accesso ai locali tecnologici;
- Protezione di tutte le porte di accesso alle dataroom.
- Protezione di tutte le aree di ricevimento merci;
- Protezione di tutte le aree di movimentazione merci, corridoi, etc.

Nella Control Room di sicurezza saranno presenti più monitor con la visualizzazione in continuo delle aree più sensibili. Il sistema di videosorveglianza dovrà essere interfacciato con il sistema antintrusione e controllo accessi in modo che qualsiasi anomalia su questi sistemi attivi ed evidenzi l'immagine del varco e/o area laddove l'anomalia è stata rilevata.

5.2.8 Architetture di rete

5.2.8.1 *Rete di distribuzione primaria ingresso provider*

L'infrastruttura del Data Center garantirà almeno due ingressi dall'esterno indipendenti per le connessioni dati. I due entry point dovranno, per quanto possibile, essere in punti contrapposti dell'insediamento.

Tali punti saranno entrambi interconnessi con entrambe le Meet me rooms mediante tubazioni ovvero canalizzazioni indipendenti ed opportunamente identificate utilizzate solo per questo scopo.

5.2.8.2 *Rete di distribuzione secondaria*

Dai due locali Meet me room ad ogni dataroom saranno presenti canalizzazioni e/o percorsi disponibili per le interconnessioni dati. Conformemente al rating, tali percorsi saranno realizzati in compartimenti antincendio diversi ed indipendenti fino all'ingresso delle dataroom stesse.

5.2.8.3 *Locali Meet me room*

I locali Meet me room rappresentano i punti di sbarco dei vari provider. Saranno presenti almeno due Meet me room per il Data Center. I due locali dovranno essere indipendenti e compartimentati tra loro. Dalle Meet me room dovrà essere possibile raggiugere qualsivoglia dataroom con l'utilizzo delle canalizzazioni di distribuzione secondaria sopra descritte.