Polo Strategico Nazionale

Shared Security Responsibilities – Schede di Servizio

Public Cloud PSN Managed Oracle

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Oracle Public Cloud PSN Managed

Il Public Cloud PSN Managed è un modello di servizio corrispondente al Public Cloud del CSP – conosciuto anche come Hyperscaler – ma permette di implementare una **doppia separazione logica e fisica**: una per la gestione operativa del servizio e una per il rilascio e il controllo sulle procedure di rilascio software.

Tra i plus del servizio Public Cloud PSN Managed c'è sicuramente la gestione totale e professionale del team di Polo Strategico Nazionale, che da un punto di vista tecnico permette:

- **Gestione dei servizi:** effettuata dallo staff certificato di Polo Strategico Nazionale sulle specifiche tecnologie messe a disposizione da Oracle (Alloy).
- **Gestione dei controlli:** il personale di Polo Strategico Nazionale analizza il rilascio di funzionalità e pacchetti software prima della loro applicazione. Nella gestione è incluso l'audit del codice, l'accesso alla telemetria di sicurezza e tutti gli strumenti per applicare e monitorare l'implementazione dei controlli**.**
- **Audit sulle modifiche:** questa operazione comprende le classi di accesso amministrativo ai dati, le implementazioni di sistemi critici, deploy e modifiche del codice e tutte le trasformazioni operative che prevedono un'approvazione esplicita da parte di Polo Strategico Nazionale per il loro completamento.
- **Accesso da parte dei CSP**: si svolge per attività di incident ed escalation verificaton, controllato e approvato solo in casi eccezionali. Il servizio permette anche di tracciare tutte le operazioni eseguite.

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Lo scopo del presente documento è quello di identificare, per i servizi **Public Cloud PSN Managed Oracle** gli **ambiti di responsabilità rispetto alla messa in sicurezza del servizio Cloud**.

Con un approccio basato su **trasparenza e condivisione**, vengono elencate le aree in cui la sicurezza è garantita dal PSN, nonché poste all'attenzione le **aree in cui la sicurezza è di responsabilità della Pubblica Amministrazione Cliente**, con l'obiettivo di garantire, **attraverso un approccio basato su sinergia e collaborazione**, la sicurezza dell'intero servizio in tutto il suo ciclo di vita.

LA SICUREZZA DEL TUO SERVIZIO CLOUD E' UNA RESPONSABILITA' CONDIVISA

Polo Strategico Nazionale

Lo Shared Security Responsibility Model

Lo **Shared Security Responsibility Model (SSRM)** è lo strumento previsto all'interno della Cloud Control Matrix – dominio **«Supply Chain Management, Trasparency and Accountability»**, attraverso il quale **Cloud Service Provider e Cloud Service Customer** definiscono e regolano in che modo la responsabilità e l'accountability per la sicurezza dei dati e delle risorse venga suddivisa nell'ambito di uno specifico **servizio Cloud**.

Per ogni controllo indicato all'interno della Cloud Control Matrix (e dunque per ogni ambito di sicurezza) viene **identificata l'ownership** specificando se questa spetta al *Cloud Service Provider*, al *Cloud Service Customer* o ad una *Terza Parte*.

CSC = P.A.

Il Customer che ha sottoscritto un contratto per usufruire del servizio

CSP = PSN

Il provider che ha contrattualizzato l'erogazione del servizio

Third Party = Gestori e Fornitori

Fornitore al quale il Provider o il Customer si rivolge per l'erogazione di una specifica componente del servizio.

***Il provider** è responsabile della sicurezza «**del**» Cloud,*

***il cliente** è responsabile della sicurezza «**nel**» Cloud.*

Polo Strategico Nazionale

Definizione delle responsabilità

Al fine di poter adeguatamente comprendere le **aree di competenza del PSN e del Cliente per la sicurezza del servizio**, queste vengono inquadrate attraverso l'utilizzo della **Cloud Control Matrix elaborata in ambito CSA Star,** nonché il **modello di responsabilità condivisa** che ne consegue, del quale tale documento rappresenta una vista sintetica.

Il framework prende in considerazione **17 Domini/Aree di sicurezza**:

A&A	Audit & Assurance
AIS	Application & Interface Security
BCR	Business Continuity Management and Operational Resilience
CCC	Change, Control and Configuration Management
CEK	Cryptography, Encryption & Key Management
DCS	Datacenter Security
DSP	Data Security & Privacy
GRC	Governance, Risk & Compliance
HRS	Human Resources
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging & Monitoring
SEF	Security Incident Management, E-Discovery & Cloud Forensics
STA	Supply Chain Management, Transparency and Accountability
TVM	Threat & Vulnerability Management
UEM	Universal Endpoint Management

Definizione delle responsabilità

Al seguito di poter **identificare i punti di confine delle responsabilità**, i domini elencati vengono inoltre inquadrati sulla base dei **layer di servizio** di seguito riportati.

DATA	I dati effettivamente gestiti e processati dalle applicazioni eseguite negli ambienti Cloud.
APPLICATION	Applicazioni/processi/funzioni elaborati da parte del cliente.
RUNTIMES	Moduli eseguibili messi a disposizione del provider che possono consentire lo sviluppo di applicazioni/processi/funzioni da parte del cliente.
MIDDLEWARE	Software di intermediazione che facilitano lo sviluppo, l'esecuzione e la comunicazione fra applicazioni.
OS (Operating System)	Software di base che dialoga con le risorse hardware virtualizzate dall'hypervisor il cui scopo è quello di ospitare e gestire il software dei livelli superiori (per estensione si intendono anche le Virtual Machine e le Virtual Appliances).
HYPERVISOR	Strumento di virtualizzazione delle risorse hardware e network, attraverso il quale sviluppare l'intera dimensione logica del servizio.
HARDWARE	Risorse fisiche messe a disposizione (CPU, RAM, Spazio su disco ...).
NETWORK	Infrastruttura fisica di trasporto dei dati a supporto dell'infrastruttura di virtualizzazione (non vi rientrano le Virtual Network).
PHYSICAL	Spazi fisici che ospitano gli strumenti ed il personale che confluiscono nell'erogazione del servizio.

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Audit & Assurance

Il dominio Audit e Assurance (A&A) è progettato per supportare il CSP e il CSC nella definizione e attuazione di un **processo di gestione dell'audit** finalizzato a: la pianificazione dell'audit, l'analisi dei rischi, la valutazione dei controlli di sicurezza, la conclusione, la correzione, la generazione dei report e le revisioni di report precedenti e delle relative evidenze a sostegno.

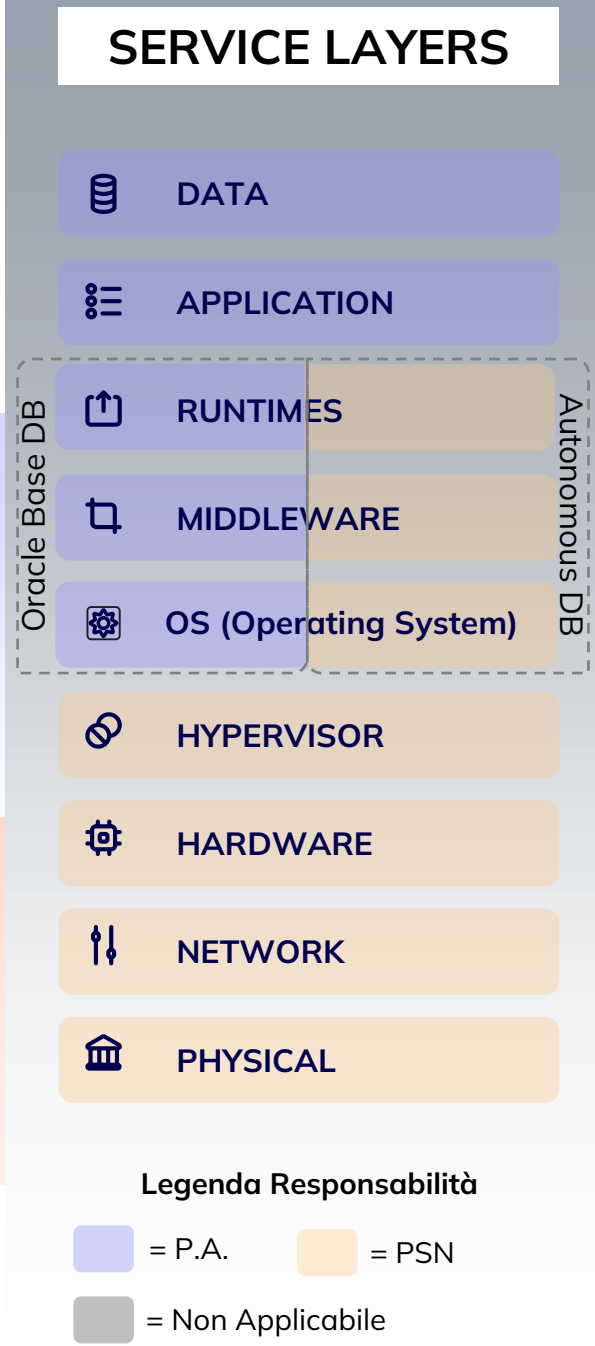
Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità del cliente svolgere attività di **audit ed assurance sulla base delle proprie esigenze di compliance ed ai controlli di propria necessità, sui workload ospitati sul servizio offerto dal PSN.**

La PA dovrà dunque elaborare le proprie politiche e procedure formali per la determinazione dello scope di analisi, degli standard rispetto ai quali svolgere le verifiche, stabilire le proprie metodologie di audit e di verifica, sulla base della propria valutazione dei rischi e delle proprie esigenze di compliance.

Responsabilità PSN (CSP)

PSN, quale organo responsabile del coordinamento e corretto funzionamento dei servizi, si occupa di svolgere attività di **audit e assurance sulle componenti di erogazione del servizio**, in linea con i service layer di competenza individuati, assicurandone la conformità ai principali standard di settore (ISO/IEC 27001, ISO 9001, ISO/IEC 20000-1, ISO 22301 e Cloud Control Matrix).



Application & Interface Security

Il dominio Application and Interface Security (AIS) è finalizzato a fornire ai CSP e CSC indicazioni relative alla **sicurezza delle applicazioni e delle interfacce (API)** nella loro progettazione, sviluppo, distribuzione. I controlli AIS aiutano le organizzazioni a identificare i rischi per gli ambienti cloud e mitigano tali rischi già nella fase di progettazione e sviluppo dell'applicazione.

Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità della P.A. cliente la **sicurezza relativa allo sviluppo di applicazioni/processi/funzioni costruiti successivamente all'acquisizione del servizio, nonché la gestione delle eventuali relative vulnerabilità.**

A tal fine è opportuno che la P.A. si doti di specifici processi/procedure per lo sviluppo sicuro, che seguano un processo SDLC definito, assegnando ruoli e responsabilità e stabilendo delle baseline per lo sviluppo, il test ed il deploy di applicazioni/processi/funzioni sviluppati.

Responsabilità PSN (CSP)

Nell'ambito dei servizi Oracle Public Cloud PSN Managed, i prodotti messi a disposizione dal cliente sono tutti **prodotti Cloud Native** progettati e sviluppati dal Cloud Service Provider partner, attraverso soluzioni di tipo tecnologico ed organizzativo che garantiscono un processo in grado di tenere in considerazione la **sicurezza delle applicazioni, dei sistemi e dei servizi in tutte le fasi del processo di sviluppo.**

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A.
= PSN
= Non Applicabile

Business Continuity Management and Operational Resilience

Il dominio Business Continuity and Operational Resilience (BCR) aiuta i CSP e i CSC a garantire che i servizi cloud siano affidabili. Il dominio guida le **strategie di continuità e resilienza**, per consentire alle organizzazioni di **continuare l'attività di fronte a interruzioni previste e impreviste**. Il dominio stabilisce i requisiti per definire il **governo della continuità** (politiche aziendali, valutare l'impatto dell'indisponibilità e dei rischi) sia **aspetti operativi** (creazione di piani di continuità operativa e la relativa documentazione, test dei piani di continuità documentati e capacità di comunicazione formale) ed **aspetti tecnologici** (capacità di **backup**, eventuali **Disaster Recovery** e ridondanze delle apparecchiature pertinenti).

Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità del cliente, in coordinamento con il PSN, sviluppare **le proprie strategie di continuità operativa relativi ai workload ospitati nel servizio offerto da PSN** in sinergia con quanto già sviluppato dal PSN, avendo cura di **determinare i propri RTO ed RPO**, attraverso un'apposita analisi degli impatti (BIA) e dei rischi (RA).

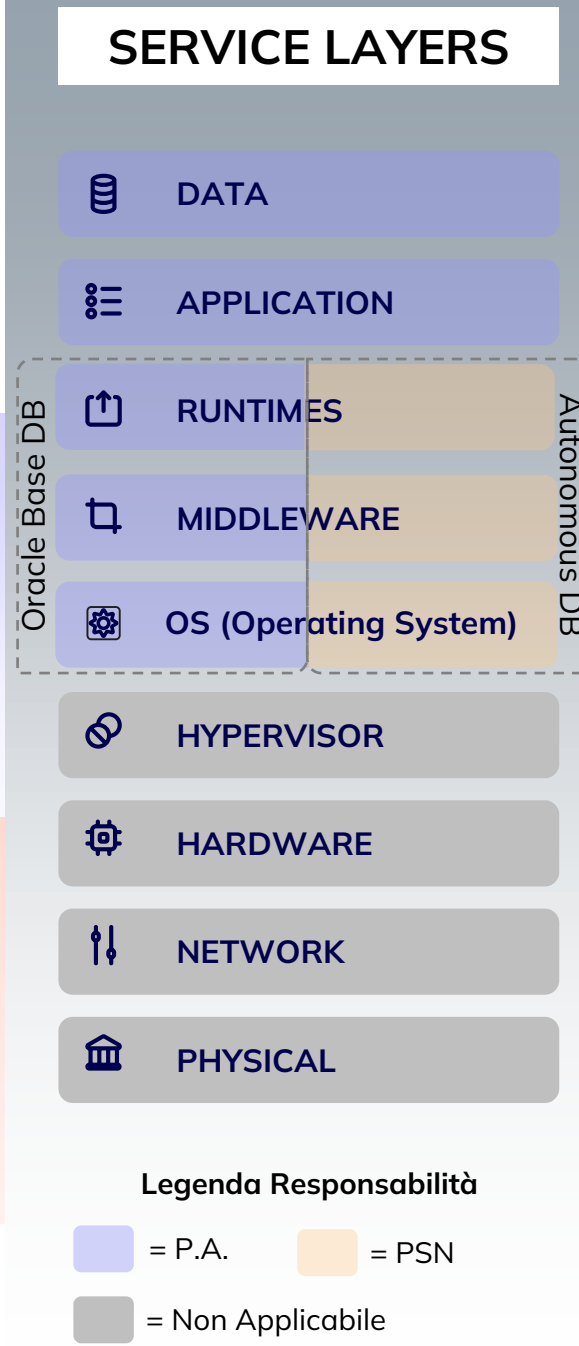
Sulla base dei propri RTO ed RPO la pubblica amministrazione gestirà gli strumenti Cloud Native di backup, sulla base del servizio acquistato, che possono essere integrati **(in termini di scope, frequenza e requisiti di sicurezza) attraverso l'acquisto del servizio Backup as a Service (BaaS)**, in linea con la tabella di compatibilità contenuta in manuale,

E' inoltre possibile fornire **soluzioni di Disaster Recovery,** oggetto di progettazione specifica nell'ambito della migrazione richiesta e formalizzate all'interno di ogni contratto con la singola PA, in dipendenza della criticità del dato stabilita dal cliente e dei relativi requisiti ACN (Determinazioni 306/2022, 307/2022 e successivi aggiornamenti) o delle specifiche esigenze espresse dai clienti, nel rispetto di quanto previsto nella Convenzione.

Responsabilità PSN (CSP)

Il PSN, in collaborazione ed in coordinamento con i propri soci gestori e gli Hyperscaler, si occupa di garantire la continuità dei servizi attraverso specifiche strategie di continuità sia di natura organizzativa che tecnologica, le quali tendono ad assicurare **la continuità e la resilienza della componente infrastrutturale del servizio.**

L'infrastruttura utilizzata è inoltre stata costruita secondo specifici requisiti di fault tolerancy e high availability, disponendo oltre che di diverse zone di disponibilità all'interno dello stesso Datacenter, anche di sviluppare apposite integrazioni su altra region, sulla base delle esigenze del cliente.



Change Control and Configuration Management.

Il dominio Change Control and Configuration Management (CCC) prevede dei controlli progettati per **mitigare i rischi associati alle change** di configurazione delle risorse informatiche (IT) mediante l'attuazione di un **processo di change management**, indipendentemente dal fatto che le risorse IT siano gestite internamente o esternamente. Questo dominio garantisce che le configurazioni delle risorse IT vengano modificate secondo specifici meccanismi di pianificazione ed approvazione.

Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità del cliente determinare il **proprio processo di change e configuration management per gestire tutte le change e le configurazioni che riguardano il proprio tenant.**

Nell'ambito del servizio erogato, infatti, il cliente si occupa del deploy delle componenti infrastrutturali necessarie (VM, OS, DB...) utilizzando prodotti la cui sicurezza e funzionalità viene garantita direttamente da Oracle, fino al momento del deploy. **Una volta che gli elementi vengono messi in esercizio, il modello di responsabilità varia in base alla tipologia** di servizio acquistato:

- **Autonomous DB**: al cliente vengono fornite delle finestre di tempo entro le quali applicare eventuali aggiornamenti, trascorse le quali sarà Oracle direttamente ad applicare le patch e le change necessarie.

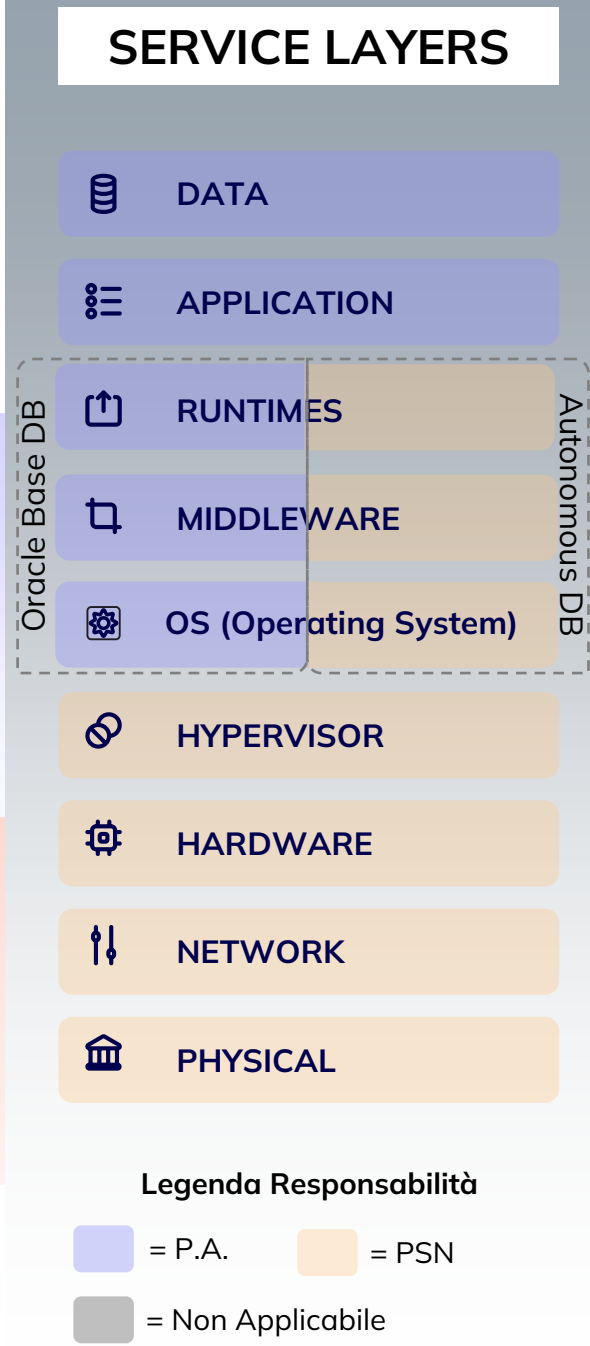
- **Altri DB**: la gestione degli aggiornamenti e della sicurezza delle componenti di servizio (VM, OS, DB) è responsabilità del cliente, il quale riceverà da parte del provider (Oracle) notifiche relative ad eventuali necessità di patching/aggiornamento, le quali dovranno però essere applicate in autonomia. Ugualmente, rimane responsabilità del cliente gestire tutte le change e le configurazioni che riguardano il proprio tenant, nell'intero ciclo di vita del servizio.

Responsabilità PSN (CSP)

E' responsabilità del PSN, per mezzo del Cloud Provider Partner Oracle, **gestire le change e le configurazioni che riguardano la componente infrastrutturale (OCI),** attraverso un processo di change management definito.

Tali attività, qualora dovessero avere impatto sui tenat cliente, vengono gestite all'interno di un'apposita finestra di manutenzione concordata.

Le change e le configurazioni relative ai tenant del cliente, seguono il modello di responsabilità descritto nella sezione CSC di cui sopra.



Cryptografy, Encryption & Key Management

Il dominio Cryptography, Encryption and Key Management (CEK) ha lo scopo di garantire che **gli algoritmi e le chiavi di cifratura vengano utilizzati per proteggere adeguatamente i dati** ospitati nel cloud e garantirne la riservatezza.

I controlli presenti in tale dominio, affrontano sia **aspetti puramente tecnologici** che **aspetti di governance, risk & compliance** per governare e gestire i rischio, elaborare il ciclo di vita delle chiavi e sistemi di gestione delle chiavi crittografiche (CKMS).

Responsabilità Pubblica Amministrazione (CSC)

Il servizio consente l'utilizzo di un paradigma Host Your Own Key (HYOK), attraverso il quale – oltre alla cifratura applicata di default «at rest» tramite strumenti Cloud Native, è possibile integrare l'utilizzo di **proprie chiavi crittografiche** attraverso KMS gestito esternamente da PSN**.**

La **chiave generata da PSN viene messa a disposizione della Pubblica Amministrazione**, alla quale spetta la responsabilità di determinare le modalità di utilizzo e il layer su cui applicare l'encytpion (compute storage, database, obj. storage).

E' inoltre responsabilità del cliente definire politiche e procedure finalizzate a determinare i **criteri di rotazione**, **disattivazione**, **duplicazione** (ecc...) delle chiavi crittografiche messe a disposizione dal provider e coordinarsi con quest'ultimo tramite apposite service request per la loro applicazione.

Responsabilità PSN (CSP)

PSN si occupa di gestire il **ciclo di vita delle chiavi crittografiche utilizzate dal cliente per la cifratura dei propri workload in coerenza con la classificazione del dato dichiarata.** Le chiavi utilizzate vengono generate tramite apposito **Key Management System (KMS).** La piattaforma KMS ha un approccio multi-tenant ed è in pieno controllo del PSN che ne è responsabile e manutentore, sia dal punto di vista sistemistico, che applicativo che per quanto concerne il ciclo di vita delle chiavi**.**

Nei servizi in ambito si applica un paradigma di HYOK, in quanto la chiave viene contenuta direttamente presso l'infrastuttura KMS gestita on prem presso i datacenter PSN e viene interrogata di volta in volta dalle componenti di servizio ospitate nel tenant cliente, sulla base di livelli di autorizzazione pre-determinati**.**

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

Datacenter Security

Il dominio Datacenter Security (DCS) specifica i requisiti relativi alla **messa in sicurezza dei Datacenter che ospitano i servizi** del cliente. I controlli presenti in tale dominio sono sempre di responsabilità del provider dell'infrastruttura, il quale si dovrà occupare di assicurare misure di sicurezza fisica ed ambientale dei Datacenter, come: controllo accessi, sicurezza perimetrale. sicurezza delle risorse hardware, corretto smaltimento di hardware dismesso ecc...

Responsabilità Pubblica Amministrazione (CSC)

La sicurezza degli ambienti fisici viene interamente gestita dal PSN e dal Cloud Service Provider partner.

Responsabilità PSN (CSP)

Il PSN, in collaborazione con il Cloud Service Provider partner Oracle , si occupa di garantire **la sicurezza dei Datacenter** che ospitano la Region Cloud di Oracle dedicate, attraverso, a titolo esemplificativo e non esaustivo:

- l'adeguata sorveglianza dei locali;
- meccanismi di controllo e limitazione degli accessi fisici;
- Gestione, manutenzione e sicurezza degli ambienti (temperatura, sistemi anti incendio, safety dei luoghi);
- Etc...

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

Data Security & Privacy

Il dominio Data Security and Privacy contiene dei controlli sulla **privacy e sulla sicurezza dei dati durante il loro intero ciclo di vita**. Questi controlli non sono specifici dell'industria o del settore e non si concentrano su un particolare paese o normativa, tuttavia sono stati sviluppati considerando gli elementi comuni e i requisiti delle principali normative sulla privacy.

Responsabilità Pubblica Amministrazione (CSC)

E' di responsabilità della Pubblica Amministrazione la **gestione dell'intero ciclo di vita del dato e dell'informazione trattata all'interno degli ambienti acquistati.** E' infatti onere del cliente in primis **classificare adeguatamente il dato in fase di on-boarding** (per garantire l'applicazione degli adeguati meccanismi di tutela) e successivamente avere un inventario delle informazioni contenute nel cloud, catalogarle sulla base della loro sensibilità, valutare gli impatti di una loro potenziale diffusione o deterioramento, periodo di retention, modalità di cancellazione ed, in generale, tutti gli accorgimenti che si ritengono necessari per la gestione dei propri dati sulla base delle proprie esigenze di compliance e di sicurezza.

Responsabilità PSN (CSP)

Tenuto conto che i servizi in ambito sono stati progettati secondo principi di Privacy e Security by Design, è compito del PSN in collaborazione col Cloud Service Provider partner, **fornire al cliente gli strumenti per la gestione dei propri dati.**

Per informazioni più dettagliate, si rimanda alla «Nomina a Responsabile del Trattamento» che PSN ha sottoscritto con la PA.

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

Governance, Risk & Compliance

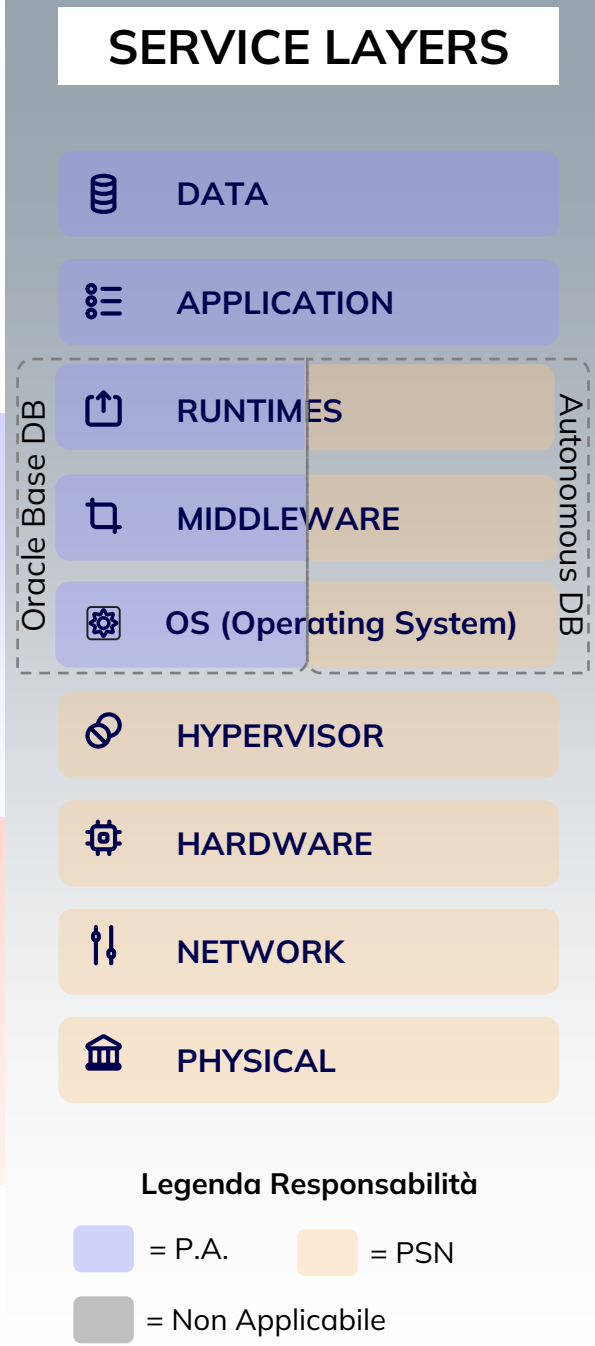
Il dominio Governance, Risk e Compliance (GRC) ha lo scopo di fornire i requisiti per **supportare, definire e dirigere gli sforzi di sicurezza e conformità** (in particolare governance aziendale e IT). L'obiettivo del dominio GRC è **fornire indicazioni per tutti i livelli di sicurezza comunemente gestiti da un comitato di governance o da un consiglio di amministrazione.** Questo dominio è strutturato per sviluppare, implementare e documentare **politiche di sicurezza** (normative, consultive e informative), **programmi di governance e rischi aziendali**, standard, baselines, linee guida e procedure per soddisfare la conformità riducendo i rischi e le vulnerabilità con l'implementazione dei controlli di sicurezza .

Responsabilità Pubblica Amministrazione (CSC)

La Pubblica Amministrazione è responsabile di implementare i **propri programmi di Governance, le proprie valutazioni del rischio e i propri sistemi di Compliance**, sulla base delle proprie esigenze normative e dei propri obiettivi.

Responsabilità PSN (CSP)

Il PSN dispone della **propria struttura di Governance**, responsabile nei vari ambiti di assicurare l'adeguato commitment e leadership delle proprie strutture e dei soci gestori, definendo al proprio interno ruoli e responsabilità, nonché la produzione di politiche e procedure necessarie alla corretta realizzazione del servizi**.** Viene svolto in tale contesto anche attività di valutazione del rischio nei vari ambiti, messi a fattor comune dall'**Enterprise Risk Management**, nonché la tenuta in considerazione dei vari **regolamenti e standard rispetto ai quali il PSN si accerta di rimanere compliant.**



Human Resources

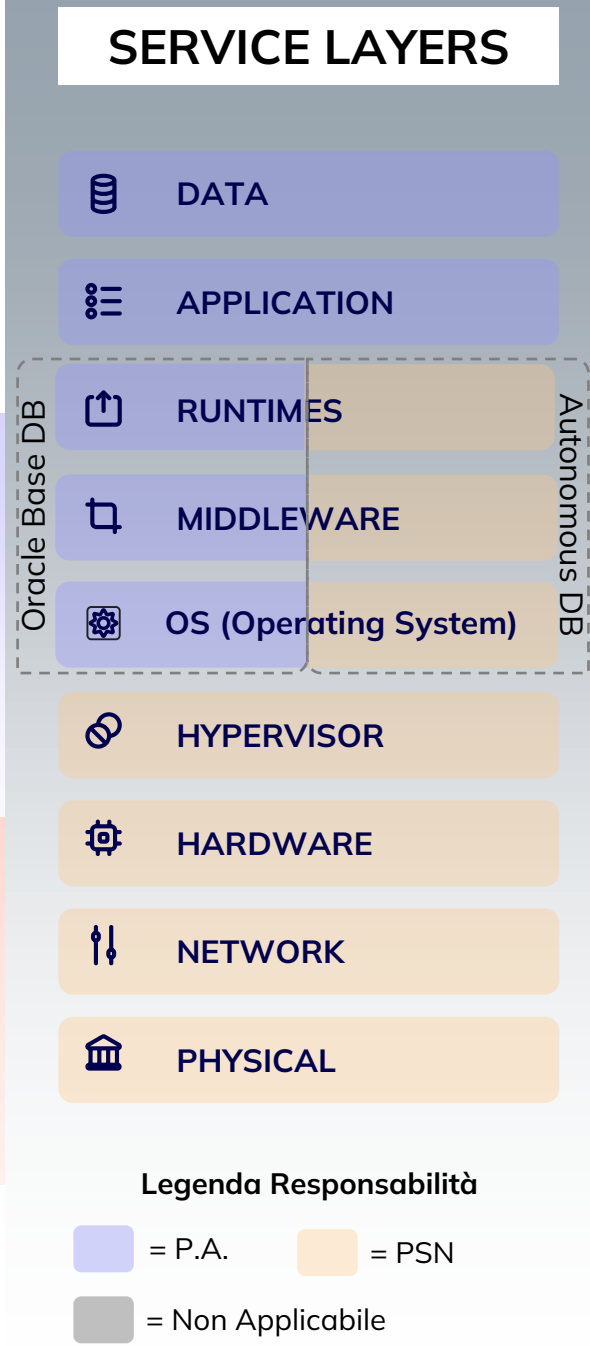
Il dominio Human Resources (HRS) definisce i **requisiti** per far sì che **il personale rispetti le politiche di sicurezza.** Gli elementi chiave del dominio delle risorse umane includono, ma non sono limitati a, screening dei precedenti del personale, contenuto del contratto di lavoro, onboarding dei dipendenti, comunicazione di ruoli e responsabilità, formazione sulla consapevolezza della sicurezza, codice di condotta e uso accettabile della strumentazione aziendale, procedure di lavoro a distanza, procedure di cambio nel ruolo di lavoro, allontanamento dei dipendenti e restituzione degli asset aziendali.

Responsabilità Pubblica Amministrazione (CSC)

E' opportuno per la pubblica amministrazione cliente assicurarsi che **il personale che adopera il servizio acquistato (sia interno che di terza parte)** sia adeguatamente formato sia in termini di capacità che sicurezza, attraverso specifici percorsi formativi e di awareness, assicurandosi di attenzionare i requisiti di sicurezza e di competenza nell'intero ciclo di vita del rapporto lavorativo (screening all'ingresso, accordi di non divulgazione, formazione sull'utilizzo degli asset aziendali e sulla gestione delle informazioni trattate ecc...).

Responsabilità PSN (CSP)

E' responsabilità del PSN assicurarsi che **il proprio personale e quello dei soci gestori impiegato nell'erogazione del servizio sia adeguatamente gestito e formato,** sia in termini di capacità e conoscenze, che di sicurezza.



Identity & Access Management

Il dominio Identity and Access Management (IAM) riguarda processi e best practice tecniche **per gestire e implementare in modo sicuro i diritti di accesso privilegiati e non privilegiati alle risorse cloud,** attraverso i principi di privilegi minimi e del controllo degli accessi basato sui ruoli. Inoltre, il dominio IAM copre **aspetti tecnici e requisiti organizzativi** per garantire che le singole entità di rete come utenti e dispositivi) abbiano accesso alle risorse pertinenti al momento giusto per le ragioni giuste.

Responsabilità Pubblica Amministrazione (CSC)

La Pubblica Amministrazione cliente è responsabile della **gestione delle identità e dei privilegi di accesso relativi alle utenze generate in autonomia** attraverso le utenze di referenza create da PSN**.** Le utenze generate della PA saranno **utenze interne allo IAM PSN**, le quali e **federate su Oracle. I** relativi privilegi potranno essere assegnati sulla base di gruppi e ruoli predefiniti.

Realizzando la federazione, tra lo IAM dell'Oracle Cloud e l'IdP del PSN, ogni user può utilizzare le sue credenziali (già esistenti nei sistemi del PSN) per accedere alle risorse di Oracle Cloud - in questo modo è possibile gestire in modo centralizzato utenze e gruppi di un'organizzazione.

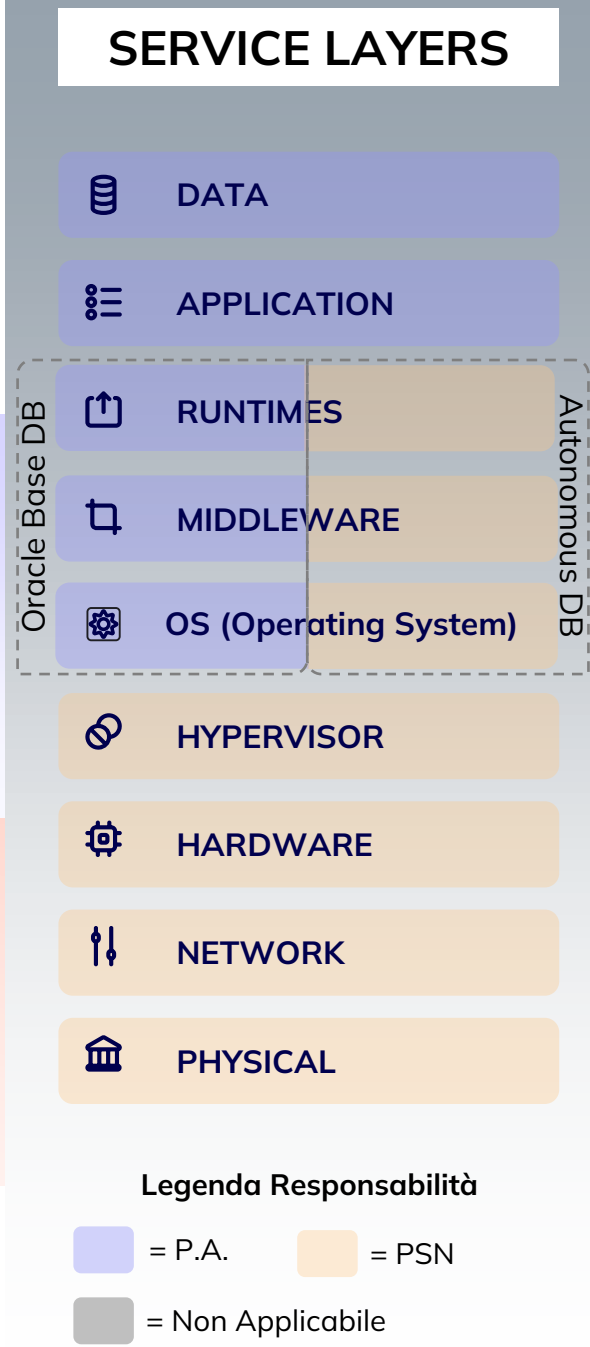
E' dunque responsabilità della PA, assicurare il **monitoraggio dell'intero ciclo di vita di queste utenze generate in autonomia**, attraverso adeguate attività di provisioning, deprovisioning, campagne di bonifica, monitoraggio attivo dei privilegi concessi e di adeguata separation of duties, nonché garantendo gli adeguati livelli di autenticazione ed accountability.

Responsabilità PSN (CSP)

PSN governa e gestisce le identità e gli accessi relativi alle **risorse utilizzate per l'erogazione del servizio e per il personale operativo del servizio**, le quali vengono federate sotto IAM PSN, assicurandone l'adeguata distribuzione di privilegi ed il monitoraggio durante l'intero ciclo di vita. E' anche responsabilità PSN garantire che l'accesso alle risorse cloud da parte di queste utenze avvenga in maniera sicura e adeguatamente monitorata.

E' inoltre responsabilità di PSN generare **due utenze, una tecnica e una amministrativa, ai referenti della PA** (censite su IAM PSN) attraverso le quali la PA sarà in grado di gestire in autonomia la creazione di altre utenze per l'accesso ai propri workload e gli aspetti economici del servizio.

L'utenza tecnica (ed eventuali utenze secondarie associate) vengono federate su Oracle Cloud, consentendone l'accesso diretto.



Interoperability & Portability

Il dominio Interoperabilità e portabilità (IPY) affronta l'**interoperabilità e la portabilità nell'ambiente cloud**. L'interoperabilità è il requisito che i componenti di un sistema di elaborazione lavorino insieme per raggiungere il risultato previsto. Inoltre, dovrebbe essere possibile che il sistema continui a funzionare se gli elementi vengono sostituiti con nuovi o diversi parti di altri fornitori. La portabilità consente ai componenti delle applicazioni e dei dati di continuare a funzionare allo stesso modo quando vengono spostati da un ambiente cloud a un altro senza subire modifiche.

Responsabilità Pubblica Amministrazione (CSC)

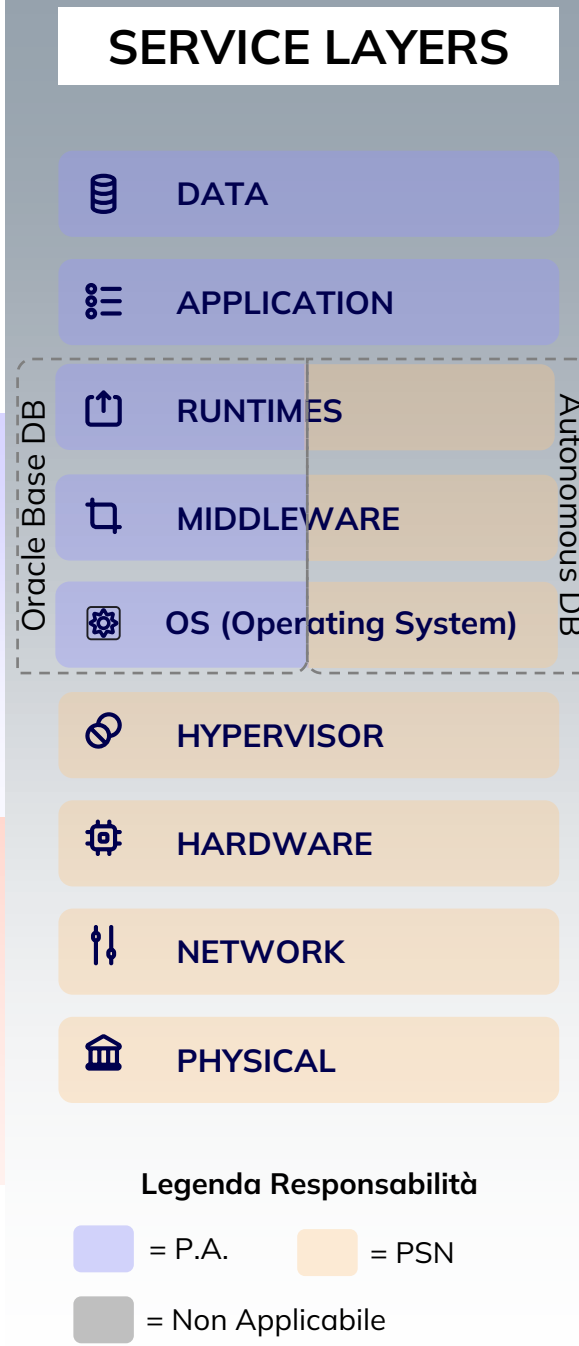
La Pubblica Amministrazione cliente è responsabile di assicurarsi che eventuali componenti applicative integrate nei DB forniti, eventuali strumenti esterni di trasformazione ed interoperabilità del dato, nonché eventuali componenti sviluppate all'interno del DB messo a disposizione, siano caratterizzati da caratteristiche di interoperabilità e portabilità. Ciò al fine di assicurarsi che un eventuale futura migrazione ad altro Provider non comporti l'inutilizzabilità dei servizi/strumenti ospitati per ragioni di incompatibilità tecnologica.

Inoltre è responsabilità della P.A., quando utilizza le stringhe di connessione messe a disposizione dal provider, di utilizzare **canali di comunicazione opportunamente cifrati (es. VPN)** per l'accesso al servizio (anche ai fini di consentire l'eventuale export di dati in modalità sicura).

Responsabilità PSN (CSP)

PSN è responsabile della fornitura al cliente di prodotti sviluppati dal Cloud Service Provider partner secondo criteri di interoperabilità e portabilità, tali da fornire al cliente del servizio gli strumenti necessari per la creazione di elementi agilmente portabili e idonei all'interoperabilità con altri ambienti, grazie all'utilizzo di **tecnologie e protocolli standardizzati.**

Il servizio erogato è infatti dotato delle API native di Oracle che consentono di mettere in comunicazione il servizio verso l'esterno, nonché di fare l'export dei propri dati in formati standard (CSV, JSON, XML...).



Infrastructure & Virtualization Security

Il dominio Infrastructure and Virtualization Security (IVS) guida i CSP e i CSC nell'implementazione dei controlli per **proteggere le infrastrutture e le tecnologie di virtualizzazione.** L'infrastruttura comprende tutto l'hardware, il software, le reti, le strutture, ecc., necessari per fornire servizi IT. Le tecnologie di virtualizzazione utilizzano il software per creare uno strato di astrazione sull'hardware del computer che consente di suddividere gli elementi hardware (come processori, memoria, spazio di archiviazione, ecc.) in computer virtuali.

Responsabilità Pubblica Amministrazione (CSC)

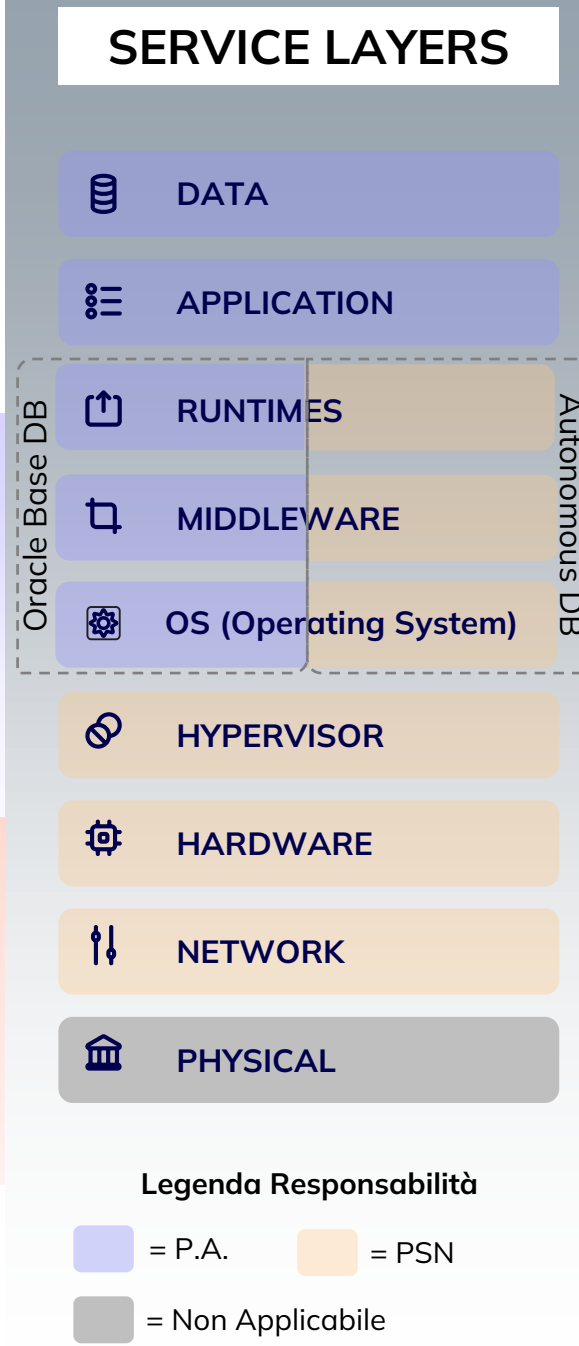
Una volta che gli elementi vengono messi in esercizio, il modello di responsabilità varia in base alla tipologia di servizio acquistato:
- **Autonomous DB**: al cliente vengono fornite delle finestre di tempo entro le quali applicare eventuali aggiornamenti, trascorse le quali sarà Oracle direttamente ad applicare le patch necessarie, per garantire livelli di sicurezza appropriati.
- **Altri DB**: la gestione degli aggiornamenti e della sicurezza della componente infrastrutturale (VM, OS) è **responsabilità del cliente**, il quale riceverà da parte del provider (Oracle) notifiche relative ad eventuali necessità di patching/aggiornamento, le quali dovranno però essere applicate in autonomia.

Inoltre, In fase di progetto dei fabbisogni la Pubblica Amministrazione Cliente può richiedere l'**abilitazione di un canale di connessione privato**, che metta in comunicaizone il proprio tenant presente su Datacenter PSN, verso eventuali altri propri tenant on prem. In alternativa, è possibile attivare attraverso la piattaforma OCI dei canali site-to-site VPN.
E' responsabilità della Pubblica Amministrazione Cliente, inoltre, **determinare le destinazioni dei vari ambienti** (test, produzione...) o attraverso la funzione di Compartment fornita dai servizi Oracle, o attraverso l'acquisizione di un ulteriore tenant, separato da quello di esercizio. Allo stesso modo, è sempre responsabilità cliente **classificare i propri ambienti** sulla base del livello di classificazione del dato contenuto.

Responsabilità PSN (CSP)

PSN è responsabile della **gestione del data center** che ospita la **Dedicate Region Cloud at Customer di Oracle**, dei DC on-premises, del supporto alle operazioni dei clienti e della gestione dei controlli di sicurezza attraverso personale dei Soci Gestori, mentre la **gestione dell'infrastruttura a servizio di Oracle Alloy** sarà affidata direttamente ad operatori Oracle operanti in UE.

Pertanto, PSN per mezzo dei soci gestori e del Cloud Provider Partner, si occuperà di garantire la sicurezza dell'infrastruttura di hosting e delle componenti infrastrutturali che potranno comporre il tenant cliente. E' infatti la **PA cliente** che si occupa **del deploy delle componenti infrastrutturali necessarie** (VM, OS...) utilizzando **prodotti la cui sicurezza viene garantita direttamente da Oracle**, fino al momento della messa in esercizio. La responsabilità relativa alla manutenzione di tali componenti, è specificata nel campo CSC.



Logging and Monitoring

Le attività di Logging e Monitoring (LOG) rappresentano un processo critico delle operazioni di sicurezza. I controlli in questo dominio enfatizzano la governance e il processo per fornire alle organizzazioni i mezzi per **realizzare registrazioni e monitoraggio efficienti**. I registri di sistemi operativi, dei servizi e delle applicazioni, svolgono un ruolo cruciale nella gestione e risposta agli incidenti, nell'analisi forense digitale e nella formazione di una visione olistica dei processi e delle risorse aziendali. La registrazione è necessaria per garantire il «non ripudio», mentre il monitoraggio e gli avvisi aiutano a fornire risposte tempestive agli incidenti di sicurezza.

Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità della Pubblica Amministrazione Cliente predisporre **il proprio processo di monitoraggio al fine di mantenere sotto controllo e registrare gli eventi relativi alle componenti contenute sopra al servizio cloud acquistato, con particolare focus alla componente applicativa,** prevedendo adeguati meccanismi di analisi e conservazione dei log, nonché di comunicazione di eventuali alert alle parti interessate sulla base delle proprie esigenze, vincoli ed obiettivi di business.

Tutti i log di sicurezza generati in OCI che sono compatibili col modello di shared responsability vengono raccolti ed esposti alla piattaforma SIEM del PSN. I log inviati al PSN sono una copia di quelli prodotti all'interno del **compartment dedicato** della PA, per cui **anche la PA stessa mantiene la visibilità su questi log tramite il servizio nativo Log di OCI** e può valutare di implementarvi i propri meccanismi di monitoraggio e gestione, paralleli a quelli del PSN.

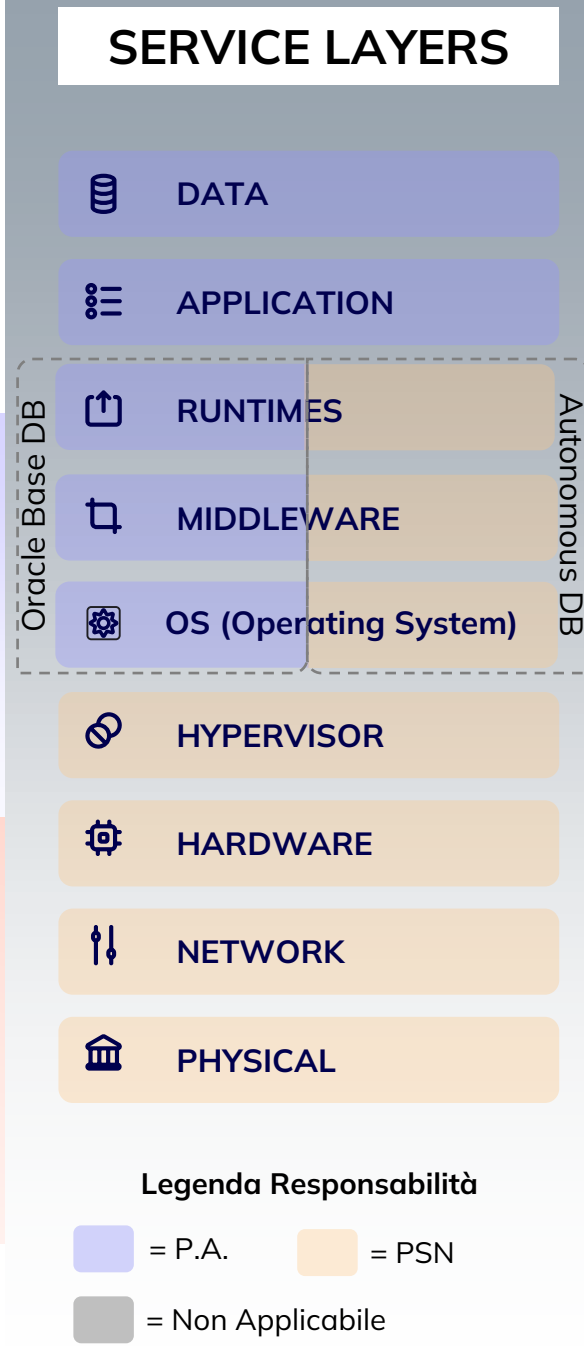
Responsabilità PSN (CSP)

PSN, per mezzo dei Soci Gestori di competenza, definisce politiche e procedure per la **raccolta e la gestione dei log di sicurezza relativi all'infrastruttura OCI che ospita il cliente**.

L'utente finale avrà l'accesso esclusivo ai dati ed ai log applicativi, gli operatori PSN avranno accesso ai log di sicurezza in caso di audit mentre gli operatori Oracle non avranno alcun accesso ai dati

Tra i diversi log disponibili lato Oracle Cloud (es. Audit log, Security Log), saranno collezionati tutti quelli relativi alla componente infrastrutturale del servizio, ad esclusione della componente applicativa, e analizzati attraverso SIEM PSN.

In ogni caso, è responsabilità della PA monitorare i log relativi ai workload ospitati all'interno del servizio.



Security Incident Management E-Discovery & Cloud Forensics

Il dominio Security Incident Management, E-Discovery e Cloud Forensics (SEF) prevede un set di controlli progettati per garantire che le policy stabilite e le procedure testate siano attuate per **rispondere adeguatamente agli incidenti di sicurezza** per mitigare i rischi aziendali (compresi eventuali requisiti per le notifiche di violazione della sicurezza).

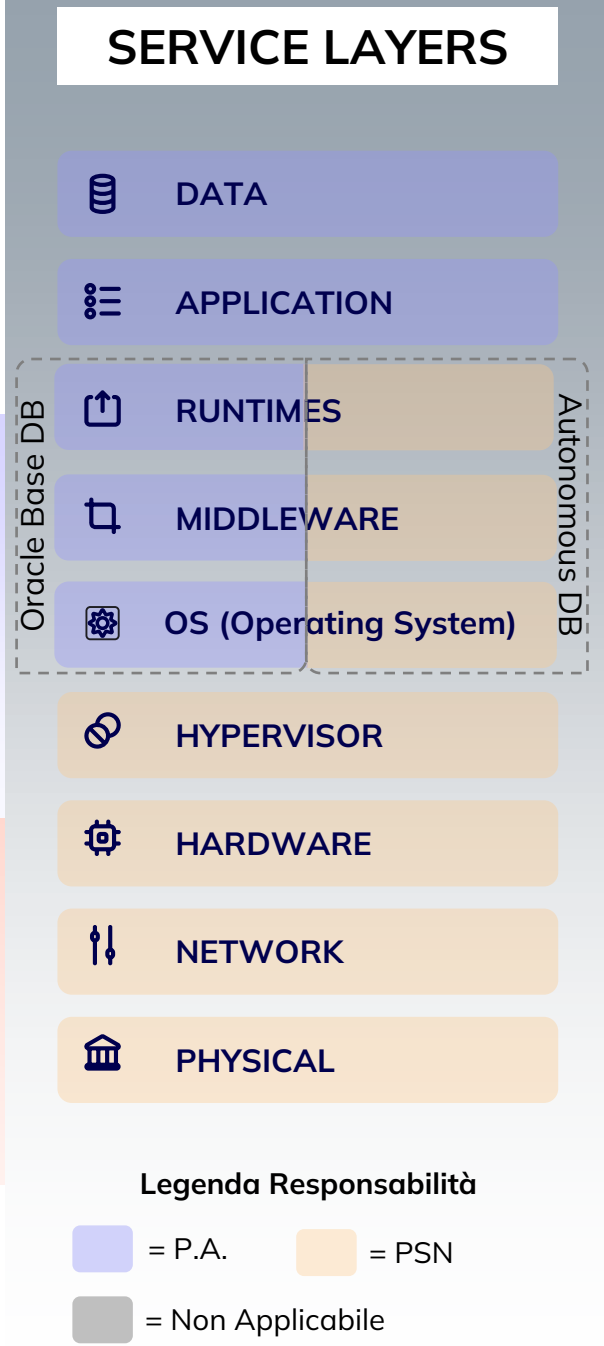
Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità della Pubblica Amministrazione Cliente gestire incidenti di sicurezza, attività di e-discovery e cloud forensics per le **componenti applicative del proprio servizio**, nonché per **eventuali componenti infrastrutturali di propria competenza**, in linea con il servizio acquistato ed il relativo modello di responsabilità.

Più in generale, la PA cliente è responsabile di gestire gli incidenti relativi al perimetro di monitoraggio di propria competenza, così come specificato nel dominio di «Logging and Monitoring».

Responsabilità PSN (CSP)

Il **Cloud Service Provider partner è responsabile di gestire gli incidenti relativi all'infrastruttura** che ospita il servizio. PSN, per mezzo dei soci gestori di competenza, si assicura di gestire gli **incidenti di sicurezza relativi alla componente infrastrutturale del servizio**, in linea con il perimetro di monitoraggio chiarito nel dominio di «Logging and Monitoring».



Supply Chain Management, Transparency and Accountability

Il dominio Supply Chain Management, Transparency and Accountability (STA) delinea un ampio insieme di controlli di **gestione del rischio della catena di fornitura**, compresi i requisiti per: definizione e gestione dell'SSRM tra il CSP e il CSC, i fornitori di terze parti utilizzano misure di sicurezza adeguate per proteggere la riservatezza, l'integrità e la disponibilità di informazioni, applicazioni e servizi nell'intero stack tecnologico, politiche e procedure per il monitoraggio e la gestione della sicurezza e della conformità lungo tutta la catena di fornitura.

Responsabilità Pubblica Amministrazione (CSC)

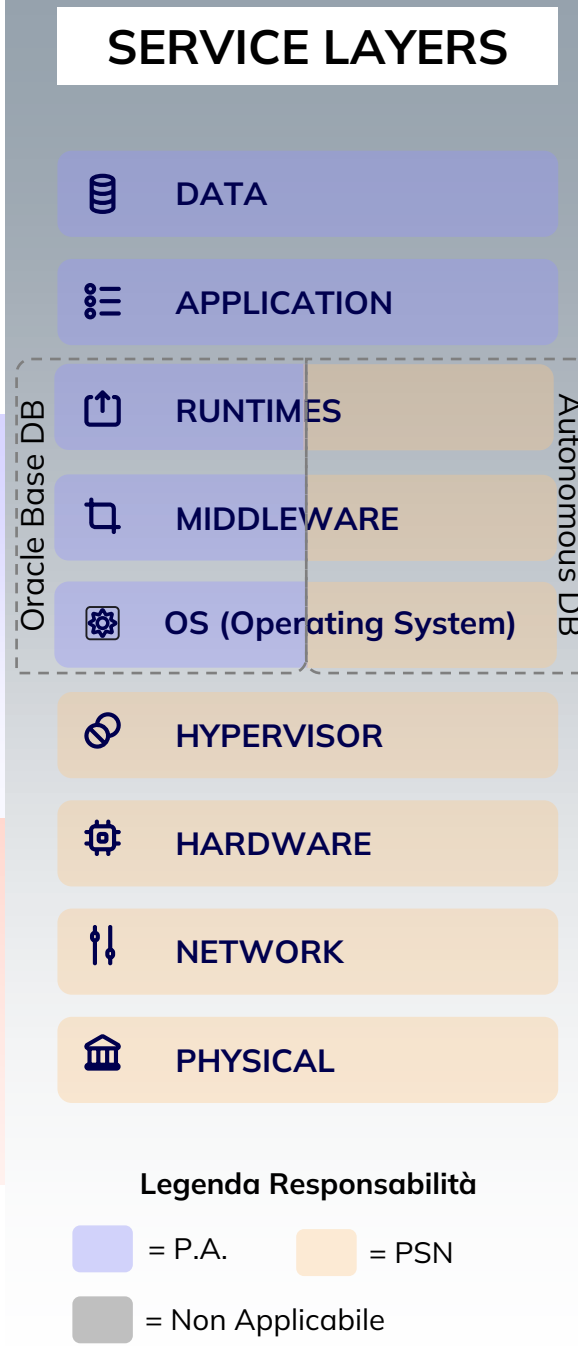
E' responsabilità della Pubblica Amministrazione Cliente **definire i propri modelli di responsabilità (Shared Security Responsibility Model)** al fine di **gestire e regolare la sicurezza relativa alle terze parti coinvolte negli ambiti di servizio di propria competenza.**

Essendo responsabilità del Cliente la gestione degli ambienti virtuali costruiti al di sopra dell'infrastruttura, ogni fornitore/terza parte coinvolto in attività in tale ambito (es. sviluppatori di software, servizio esterno di security monitoring ...) è opportuna che venga gestito dalla Pubblica Amministrazione secondo i propri modelli di gestione di sicurezza delle terze parti, in accordo a quanto previsto dai controlli contenuti nel presente dominio di sicurezza.

Responsabilità PSN (CSP)

E' responsabilità del PSN **gestire le terze parti che concorrono all'erogazione del servizio (fra le quali rientrano anche i soci gestori** che si occupano della concreta erogazione del servizio) assicurandosi di **definire e comunicare adeguatamente le porzioni di responsabilità** all'interno del servizio attraverso un modello di **responsabilità condivisa della sicurezza (Shared Security Responsibility Model** – di cui il presente documento rappresenta una guida riepilogativa).

Il PSN, **per le terze parti coinvolte nelle componenti infrastrutturali del presente servizio**, si occupa di definirne le responsabilità, monitorarne le attività, gestirne i rischi associati.



Threat & Vulnerability Management

Il dominio Threat and Vulnerability Management (TVM) si concentra **sulla valutazione e sulla mitigazione delle vulnerabilità** che potrebbero evolversi e avere un impatto su risorse, architetture di sicurezza, progetti e componenti della soluzione. La gestione delle vulnerabilità dovrebbe essere affrontata attraverso specifiche politiche/procedure/misure tecniche, strategie per l'individuazione e la gestione delle vulnerabilità, implementazione di specifici strumenti di detection (basati sull'individuazione di specifiche threat signatures), svolgimento di penetration tests ecc...

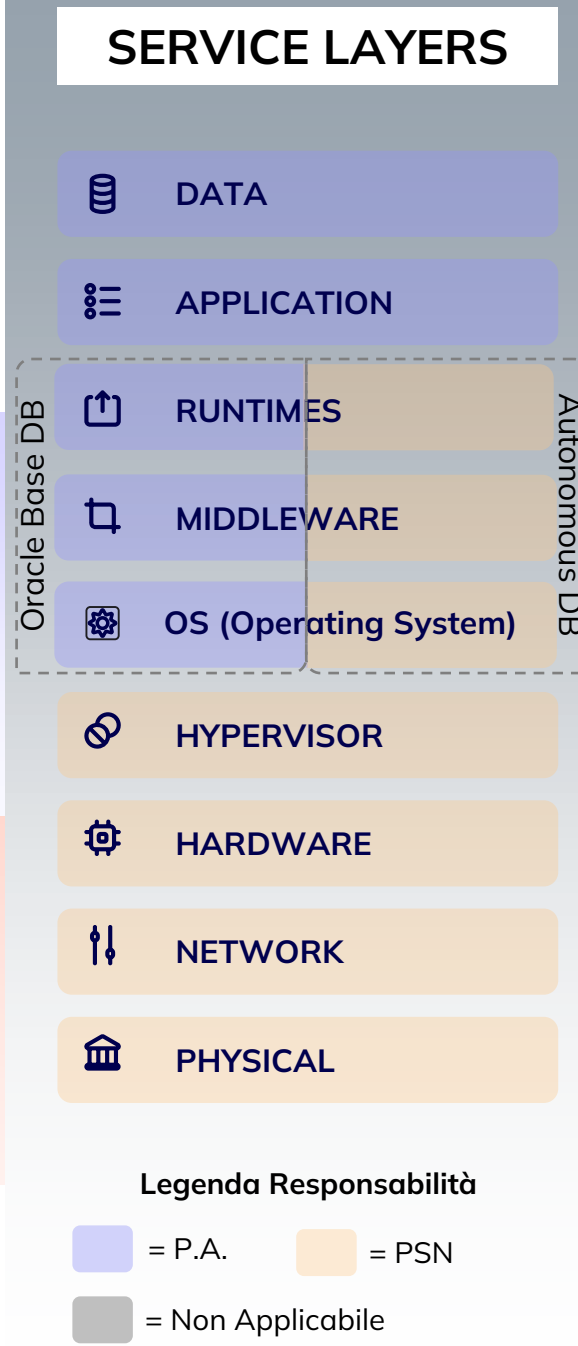
Responsabilità Pubblica Amministrazione (CSC)

E' responsabilità della Pubblica Amministrazione Cliente **predisporre il proprio processo di identificazione e gestione delle vulnerabilità e delle minacce**, assicurandosi di porre in essere attività di **malware protection, patching, VA e PT, per tutti gli elementi contenuti all'interno del proprio tenant.**

Responsabilità PSN (CSP)

E' responsabilità del PSN per mezzo dei Soci Gestori e del Cloud Service Provider partner, **gestire le vulnerabilità che riguardano gli elementi infrastrutturali della componente di compartment di servizio** (elementi network, elementi di gestione di eventuale Backup as a Service ed – in generale – elementi a contorno del tenant cliente), assicurandosi oltre che di porre in essere un'adeguata **malware protection,** di individuare tempestivamente e gestire attraverso apposite attività di **patching** eventuali vulnerabilità che interessano l'infrastruttura, secondo specifiche metriche di rischio (anche attraverso campagne periodiche di **Vulnerability Assessment e Penetration Testing**).

Il processo è gestito tramite i due documenti, il primo riguarda assessment periodici (VA e PT) mentre il secondo riguarda una gestione preventiva e proattiva delle vulnerabilità presenti in scope. L'asset owner che riceve come input la vulnerabilità riscontrata la riceve e ne pianifica e applica remediation secondo processo di Change Management di PSN.



Responsabilità: Condivisa PSN e PA

Universal Endpoint Management

Il dominio Universal Endpoint Management (UEM) si concentra sull'implementazione dei controlli per **mitigare i rischi associati all'utilizzo di un computer all'esterno dell'ufficio**, inclusi i dispositivi mobili e i dispositivi endpoint in generale. Riguarda principalmente il **comportamento degli utenti e la consapevolezza** (o la mancanza di consapevolezza) dell'approccio di un'azienda all'uso accettabile di dispositivi e tecnologie (ad esempio, gestiti o non gestiti, di proprietà aziendale o personali). Il dominio si occupa di: mantenimento di un inventario di tutti gli endpoint, l'approvazione di servizi e applicazioni accettabili per l'uso da parte degli endpoint, l'implementazione di misure di sicurezza come schermate di blocco automatiche, firewall e rilevamento anti-malware e utilizzando tecnologie di prevenzione, crittografia dell'archiviazione e tecnologie di prevenzione della perdita di dati.

Responsabilità Pubblica Amministrazione (CSC)

La PA cliente deve assicurarsi di porre in essere **processi/procedure/soluzioni tecnologiche per la gestione sicura dei propri endpoint**, tali da assicurare un controllo capillare e tempestivo dei dispositivi utilizzati per la fruizione del servizio.

In termini processivi/procedurali, sarebbe opportuno definire un governo di tali attività che si occupi tanto dell'awareness degli utenti, quanto della definizione dei requisiti e delle policy di sicurezza da adottare rispetto agli endpoint in scope.

Da un punto di vista tecnologico, sarebbe opportuno dotarsi di soluzioni di tipo MDM o DLP, per garantire l'hardenizzazione e la gestione centrale dei propri endpoint.

Responsabilità PSN (CSP)

PSN si occupa di **gestire e regolare la sicurezza relativa agli endpoint propri e dei soci gestori** utilizzati per l'erogazione del servizio, attraverso la definizione di uno specifico processo di governo e l'applicazione di apposite tecnologie (MDM, DLP...) in grado di mantenere un inventario aggiornato degli endpoint gestiti ed autorizzati, gestirne centralmente le policy, la cifratura l'anti-malware e software firewalls per la relativa protezione e l'hardenizzazione dei dispositivi in generale.

SERVICE LAYERS

- DATA
- APPLICATION
- RUNTIMES
- MIDDLEWARE
- OS (Operating System)
- HYPERVISOR
- HARDWARE
- NETWORK
- PHYSICAL

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Matrice di sintesi

A riepilogo degli ambiti di responsabilità descritti all'interno documento, è possibile riassumere che per i servizi **Oracle Public Cloud PSN Managed** la sicurezza del servizio è suddivisa secondo le seguenti aree di responsabilità:

Responsabilità Pubblica Amministrazione (CSC)

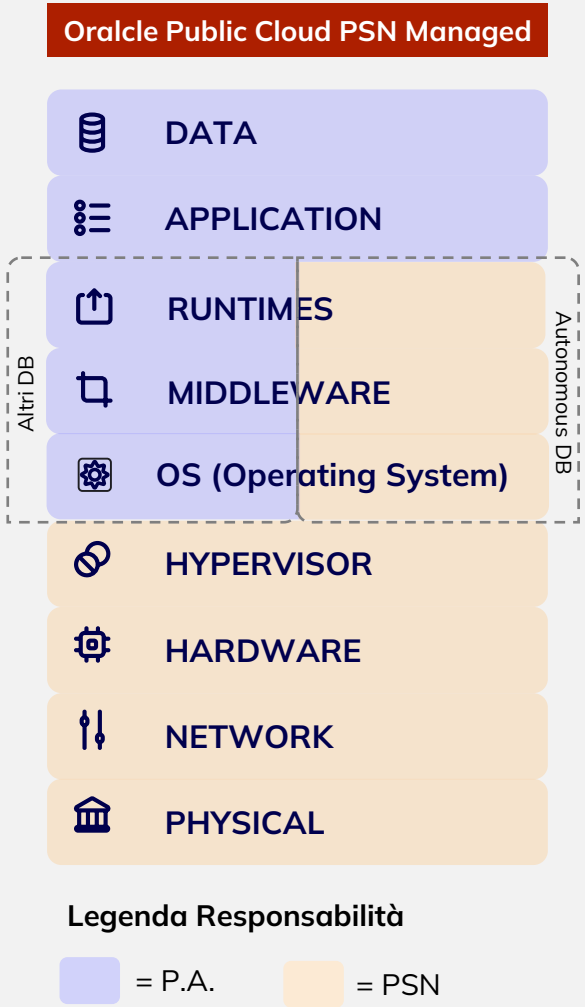
La Pubblica Amministrazione cliente è **responsabile, oltre che della messa in sicurezza delle componenti applicative integrate nel servizio e dei dati in esso contenuti**, anche della **manutenzione della sicurezza del proprio tenant (es. patching OS, patching DB, sicurezza VM o cluster VM...),** ad eccezione dei servizi Autonomous DB, per cui la sicurezza dell'infrastruttura verrà comunque garantita dal provider.

Responsabilità PSN (CSP)

PSN è responsabile della gestione del data center che ospiterà la Dedicate Region Cloud at Customer di Oracle, dei DC on-premises, del supporto alle operazioni dei clienti e della gestione dei controlli di sicurezza La gestione dell'infrastruttura a servizio di Oracle Alloy sarà affidata direttamente ad operatori Oracle operanti in UE.

Nel caso di servizi **Autonomous DB**, il provider si occupa di garantire e mantenere la sicurezza per tutta la componente infrastrutturale e sistemistica, lasciando al cliente la sola responsabilità di utilizzare i DB e eventuali elementi applicativi.

Per gli altri servizi di Database erogati, invece, **la sicurezza dell'infrastruttura viene sempre garantita da PSN in collaborazione con Oracle**, lasciando il compito di **mantenere la sicurezza su tutto il tenant al cliente (es. patching OS, patching DB, sicurezza VM o cluster VM...).**



Polo Strategico Nazionale

Cloud sicuro per l’Italia digitale.

www.polostrategiconazionale.it