Polo Strategico Nazionale

Shared Security Responsibilities – Schede di Servizio

CaaS Open Source

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Container as a Service

Il servizio **CaaS Open Source** è un servizio cloud basato su piattaforma Red Hat Openshift Container Platform.

Questa soluzione consente alle Amministrazioni di **sviluppare e gestire applicazioni cloud native** in un ambiente creato per distribuire e gestire **applicazioni containerizzate** in modo sicuro e scalabile.

L'orchestrazione dei container basata su Kubernetes garantisce un ambiente multi cloud progettato per funzionare su diverse infrastrutture, inclusi ambienti on-premises e cloud pubblici.

L'**integrazione tra Kubernetes e Red Hat** rende l'esperienza ancora più affidabile mentre **OpenShift semplifica il processo di deployment** e scalabilità delle applicazioni containerizzate. La sicurezza della piattaforma è data da funzionalità come la **scansione delle immagini dei container**, il **controllo degli accessi** basato sui ruoli (RBAC) e la **crittografia dei dati sensibili** per garantire l'integrità delle applicazioni.

Il **PSN** si occuperà della gestione dell'infrastruttura relativa al servizio, ed **alla piattaforma di containerizzazione, per consentire ai clienti la gestione di Container all'interno di un project dedicato** e consentire processi di sviluppo e distribuzione scalabili.

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 il servizio **Container as Service Open Source (CaaS OS) 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, sulle componenti applicative contenute all'interno dei container forniti 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 propria competenza del servizio**, assicurandone la conformità ai principali standard di settore (ISO/IEC 27001, ISO 9001, ISO/IEC 20000-1, ISO 22301 e Cloud Control Matrix).

L'attività si concentra sulla **componente infrastrutturale**, la quale tiene conto degli ambenti fisici, del network e dell'hardware utilizzati.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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)

La Pubblica Amministrazione Cliente è responsabile per **lo sviluppo sicuro delle applicazioni ed interfacce applicative sviluppate e/o distribuite all'interno dei propri container**, assicurandosi di avere in piedi opportuni processi (SDLC), adeguatamente proceduralizzati, che garantiscano la sicurezza durante l'intero ciclo di vita dello sviluppo (design, test, deploy, vulnerability management ecc..).

Responsabilità PSN (CSP)

PSN, quale provider responsabile solamente per la fornitura dell'infrastruttura Cloud e della piattaforma di containerizzazione non interagisce in nessun modo con gli elementi nei workload e, pertanto, non svolge alcuna attività di sviluppo.

Il servizio è infatti erogato con lo scopo di **fornire ai clienti la possibilità di gestire le proprie attività di sviluppo** in maniera strutturata e scalabile.

Tutti i requisiti di sicurezza in tale ambito, pertanto, rimangono a carico della Pubblica Amministrazione cliente.

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 strategie di continuità operativa relativa ai propri container ed alle componenti applicative ospitate.** In tale ambito sarà opportuno che il cliente sviluppi le proprie strategie in sinergia con quanto già sviluppato dal PSN in termini infrastrutturali, avendo cura di determinare i propri RTO ed RPO, attraverso un'apposita analisi degli impatti (BIA).

E' possibile per il cliente, in dipendenza della criticità del dato stabilita e dei relativi requisiti ACN (Determinazioni 306/2022, 307/2022 e successivi aggiornamenti) nel rispetto di quanto previsto nella Convenzione, **richiedere l'ampliamento del servizio in modello doppia region**, richiedendo a PSN di istanziare un ulteriore tenant all'interno della region geograficamente opposta. **Rimane responsabilità della Pubblica Amministrazione Cliente la gestione della componente applicativa del workload (sia per il tenant di esercizio che per quello di DR), dovendo prevedere** - nell'ambito delle proprie responsabilità **- degli opportuni meccanismi di replica a livello applicativo.**

Le attività di backup, invece, vengono gestite direttamente dal personale dei Soci Gestori del PSN secondo policy standard, le quali possono essere integrate e modificate in sede di progetto dei fabbisogni, in linea con gli RTO e RPO definiti dalla PA. Anche l'attività di restore, è gestita da parte del personale provider, sulla base delle richieste effettuate dalla PA per mezzo ticket.

Responsabilità PSN (CSP)

Il PSN, in collaborazione ed in coordinamento con i propri soci gestori, 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.**

E' responsabilità del PSN per mezzo dei soci gestori, **gestire i backup dei namespaces/projects del cliente**, in linea con le policy standard. Da policy di default, è previsto un backup incrementale giornaliero e un full settimanale, con periodi di retention di 7 giorni. Per maggiori informazioni relativamente agli oggetti che vengono interessati da backup e quelli che rimangono esclusi, visita: https://documentation.commvault.com/2023e/essential/backups_for_kubernetes.html.

L'architettura del servizio, inoltre, è disegnata secondo criteri di **High Availability**, prevedendo la creazione di 3 Fault Domain all'interno della region che ospita il servizio. Tutte le VM necessarie al corretto funzionamento di RedHat Openshift sono deployate all'interno del cluster VMware Stretched e utilizzano i datastore previsti. Di default il servizio viene attivato su una sola region (Nord o Sud).

Di default il servizio viene attivato su **una sola region** (Nord o Sud), ma rimane possibile per il cliente, in dipendenza della criticità del dato stabilita e dei relativi requisiti ACN (Determinazioni 306/2022, 307/2022 e successivi aggiornamenti) o delle specifiche esigenze espresse, nel rispetto di quanto previsto nella Convenzione, richiedere l'ampliamento del servizio in modello doppia region, richiedendo a PSN di istanziare **un ulteriore tenant all'interno della region geograficamente opposta.**

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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 rispetto alla gestione dei container e delle componenti applicative ospitate.**

E' dunque opportuno che la PA elabori e governi i propri processi di change e configuration management, al fine di **gestire le change e le configurazione relative ai propri ambienti**, determinandone gli impatti, i rischi rispetto alle proprie esigenze operative.

Responsabilità PSN (CSP)

E' responsabilità del PSN gestire tutte **le configurazioni e le change infrastrutturali (network e hardware), nonché le configurazioni iniziali dell'Hypervisor e sulla piattaforma di containerizzazione**, secondo apposito processo di change management che tiene conto degli impatti e dei rischi associati alle change, assicurandosi che queste vengano svolte solo da personale autorizzato e secondo metodologie consolidate, assicurandosi di stabilire specifici meccanismi di considerazione e comunicazione verso i clienti impattati dalle specifiche change.

E' inoltre responsabilità di PSN, gestire eventuali change relative al servizio del cliente, a seguito di apposita change request, per quanto riguarda **creazione nuove utenze e cancellazione del project cliente** (tali attività saranno avviate da input cliente, ma gestite esclusivamente da personale PSN)

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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)

E' possibile per la PA Cliente, sulla base del livello di criticità di dati ospitato, richiedere l'attivazione del **servizio opzionale di cifratura (EKM).**

In caso di richiesta di abilitazione del servizio di EKM, verrà configurata la comunicazione tra vCenter e EKM, che implicherà il vincolo di utilizzo di template cifrati per la generazione delle VM che ospiteranno il servizio (a carico del personale PSN). Di conseguenza, ogni VM avrà la propria chiave, il cui periodo di validità andtrà definito dal cliente. E' infatti responsabilità della Pubblica Amministrazione Cliente **definire il criptoperiodo (periodo di rotazione della chiave)** sulla base delle proprie esigenze di data protection e il proprio risk appetite, comunicandolo attraverso apposita service request al personale PSN per il relativo enforcement.

I dati in transito interni all'infrastruttura comunicano attraverso canali cifrati. Rimane responsabilità della Pubblica Amministrazione cliente assicurarsi di utilizzare **canali di comunicazione cifrati per l'interazione (sia interna che esterna) delle componenti sviluppate sul proprio workload** (container, applicazioni, eventuali API e middleware). Il servizio è esposto in modalità sicura. E' comunque auspicabile che il cliente utilizzi **meccanismi di connessione sicura per accedere al servizio**, nonché per la comunicazione fra applicazioni (vedi linee guida nei domini di AIS e IPY).

Responsabilità PSN (CSP)

PSN si occupa di gestire il **ciclo di vita delle chiavi crittografiche utilizzate dal cliente per la cifratura dei propri tenant,** 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.

Nel servizio CaaS vengono **opzionalmente cifrate la VM** (ed eventuali Container in essa contenuti) sui quali è sviluppata l'istanza cliente del servizio, assicurando la cifratura del dato "at-rest". Queste capabilities di cifratura devono essere **espressamente richieste dal cliente in fase di onboarding sulla base della classificazione dato ospitato** (in caso di dati critici o strategici, per come dichiarato in progetto di fabbisogni). In caso di richiesta del servizio, sarà il personale PSN ad occuparsi della configurazione delle componenti di cifratura direttamente sulle VM che ospitano il servizio ed applicare – di conseguenza – eventuali rotazioni di chiave sulla base delle richieste del cliente.

I dati in transito interni all'infrastruttura (comunicazione delle interfacce tra vari moduli interni al servizio) comunicano attraverso specifici canali cifrati appositamente predisposti. E' responsabilità della Pubblica Amministrazione cliente assicurarsi di utilizzare canali di comunicazione cifrati per l'interazione (sia interna che esterna) delle componenti sviluppate sul proprio workload (container, applicazioni, eventuali API e middleware). Il servizio è esposto in modalità sicura.

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.

Responsabilità PSN (CSP)

Il PSN si occupa di garantire **la sicurezza dei Datacenter che ospitano i servizi offerti**, garantendo, in descrizione sommaria:

- 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 avere un inventario delle informazioni contenute nel cloud, catalogarle sulla base della loro sensibilità, valutare gli impatti di una loro potenziale diffusione o deterioramento, applicare modalità di privacy by default alle componenti sviluppate in autonomia, definire 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 **fornire gli strumenti per la gestione dei propri dati**, i quali consistono in;

- Strumenti per la **cancellazione forense del dato** qualora necessario;
- **Inventario** degli strumenti hardware nei quali sono contenute le informazioni del CSC;
- Strumenti per **l'individuazione della posizione fisica del dato, anche nei relativi backup**.

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

Responsabilità: Condivisa PSN e PA

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 e dei propri obiettivi.

Nell'ambito dei servizi CaaS OS, **è dunque responsabilità del cliente definire Governance, Risk e Compliance per la gestione degli elementi deployati all'interno dei container**,

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.**

Nell'ambito dei servizi CaaS OS, tale attività si estende solamente agli elementi che contribuiscono all'area del servizio di propria competenza (infrastruttura e piattaforma di container), lasciando la **gestione degli altri ambiti di servizio non infrastrutturali direttamente al Customer.**

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

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, attraverso le utenze di referenza create da PSN, è responsabile della **gestione delle identità e dei privilegi di accesso relativi alle utenze generate in autonomia sulla piattaforma di containerizzazione** (attraverso il processo mediato descritto nel campo responsabilità CSP), nonché **tutte le utenze generate ed esistenti sulle componenti applicative istanziate nei container.**

E' dunque responsabilità della PA, assicurare il monitoraggio dell'intero ciclo di vita di queste utenze, 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**, le quali vengono federate sotto IAM PSN.

E' inoltre responsabilità di PNS **generare due utenze tecnico/amministrative al referente della PA.** Il referente tecnico ha possibilità di **generare in autonomia delle utenze secondarie tramite CMP PSN**, sulle quali sarà possibile abilitare accesso ad Opensihift.
Una volta generata l'utenza secondaria, per poterla abilitare all'accesso su piattaforma Openshift, sarà necessario inviare apposita richiesta via ticket al personale PSN, richiedendo abilitazione ad accesso a piattaforma, indicando i ruoli che si vogliono conferire.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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)

E' responsabilità della Pubblica Amministrazione Cliente utilizzare gli strumenti di portabilità ed interoperabilità forniti dal provider in maniera sicura.

Tenuto conto delle caratteristiche di portabilità degli applicativi consentita dal deployment su container, è invece completamente a carico del cliente assicurarsi di **utilizzare strumenti di sviluppo che garantiscano la portabilità dell'applicativo** istanziato e/o sviluppato in autonomia.

Responsabilità PSN (CSP)

Il servizio CaaS nasce con l'obiettivo di garantire ai clienti requisiti di portabilità ed interoperabilità dei propri workload.

La piattaforma messa a disposizione, infatti, è dotata di una serie di **API native**, configurate e messe in sicurezza dal personale PSN (con vincoli di accesso e protocolli sicuri), che la pubblica amministrazione può utilizzare per esportare i propri dati in maniera sicura e mettere in comunicazione verso l'esterno i propri container/applicazioni.

La piattaforma, inoltre, utilizza esclusivamente **formati standard** e garantisce la **persistenza dei dati** a livello infrastrutturale.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A.

= PSN

= Non Applicabile

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)

La Pubblica Amministrazione Cliente accede direttamente ad un'interfaccia di gestione del servizio ed è completamente astratta dalle necessità di gestire infrastruttura e sistema operativo.

La responsabilità che residua alla PA cliente è di **gestire, separare, classificare e monitorare i propri ambienti** (esercizio, test, produzione...) sulla base delle proprie esigenze operative, nonché **classificarli in linea con la tipologia di dati** in essi contenuti.

Responsabilità PSN (CSP)

Il **PSN** si occupa della gestione dell'infrastruttura relativa al servizio, ed **alla piattaforma di containerizzazione, per consentire ai clienti la gestione di Container all'interno di un project dedicato** e consentire processi di sviluppo e distribuzione scalabili.
E' dunque responsabilità di PSN gestire la componente di virtualizzazione sottesa all'infrastruttura, nonché l'hardenizzazione dei Sistemi Operativi e delle componenti di middleware relative alla piattaforma di containerizzazione, garantendo opportuna separazione e segregazione degli ambienti.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

Responsabilità: Condivisa PSN e PA

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 applicative istanziate nei container,** 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.

Responsabilità PSN (CSP)

E' responsabilità del PSN **monitorare l'infrastruttura e l'intero stack virtuale** alla base dell'erogazione del servizio, mantenendo sotto controllo gli **eventi relativi alla dimensione fisica, network, hardware, hypervisor, Sistema Operativo e piattaforma Openshift**, attraverso uno specifico processo di monitoraggio il quale ha lo scopo di **monitorare ed identificare ogni evento, raccoglierne e conservarne in sicurezza i log, identificare eventuali anomalie** e comunicarle alle parti interessate.

E' responsabilità del PSN comunicare eventuali anomalie riscontrate sugli ambienti di propria competenza, alla Pubblica Amministrazione Cliente interessata, secondo le modalità concordate.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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 predisporre **il proprio processo di monitoraggio di gestione degli incidenti, e-discovery e cloud forensic per le componenti applicative istanziate nei container**, secondo le proprie metriche di sicurezza e le proprie specifiche esigenze normative/contrattuali.

Responsabilità PSN (CSP)

E' responsabilità del PSN **gestire gli incidenti che interessano l'infrastruttura e l'intero stack virtuale** alla base dell'erogazione del servizio, gestendo gli **incident relativi alla dimensione fisica, network, hardware, hypervisor, Sistema Operativo e piattaforma Openshift** e garantire attività i e-discovery e Cloud Forensic, attraverso specifico processo di incident management (attestato conforme allo standard ISO/IEC 27035), i quali vengono periodicamente testati secondo specifiche metriche di risoluzione e che si assicurano di risolvere gli incidenti e comunicarli agli stakeholders interessati secondo criteri precedentemente concordati.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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.

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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 in autonomia attività di **malware protection, patching, Vulnerability asessment e Penetration Test per le per i container istanziati in autonomia e le componenti applicative** in questi contenute.

Responsabilità PSN (CSP)

E' responsabilità del PSN **gestire le vulnerabilità che riguardano l'infrastruttura e l'intero stack virtuale** alla base dell'erogazione del servizio **(Hypervisor, piattaforma OpenShift e relativi middleware)** 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**).

SERVICE LAYERS

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

Legenda Responsabilità

= P.A. = PSN

= Non Applicabile

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 il servizio **CaaS Open Source** la sicurezza del servizio è suddivisa secondo le seguenti aree di responsabilità:

Responsabilità Pubblica Amministrazione (CSC)

La Pubblica Amministrazione cliente è **responsabile della messa in sicurezza dei container rilasciati** sull'infrastruttura fornita da PSN durante il loro intero ciclo di vita, nonché delle **componenti applicative** in essi contenute, assicurandosi garantirne la sicurezza in tutte le fasi, a partire da quella di sviluppo.

Responsabilità PSN (CSP)

PSN è **responsabile della messa in sicurezza dell'infrastruttura** sulla quale vengono ospitati gli ambienti virtuali acquistati dalle Pubbliche Amministrazioni e della **piattaforma di containerizzazione** sulla quale vengono generate le istanze dei clienti, assicurando la **sicurezza fisica, della rete fisica, dell'hardware e dell'hypervisor** utilizzati per l'erogazione del servizio, nonché l'hardenizzazione del Sistema Operativo e delle componenti di middleware sottostanti la piattaforma di erogazione.

CaaS OS

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

Legenda Responsabilità

= P.A. = PSN

Polo Strategico Nazionale

Cloud sicuro per l’Italia digitale.

www.polostrategiconazionale.it

INTERNAL USE