Polo Strategico Nazionale

Shared Security Responsibilities – Schede di Servizio

Servizi DRaaS

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Backup as a Service

Il **Disaster Recovery “as-a-Service” (DRaaS)** è il servizio di cloud computing che consente il **ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati**. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso.

Il modello as-a-service prevede che l'amministrazione stessa non debba essere proprietaria di tutte le risorse né occuparsi di tutti gli strumenti necessari per il Disaster Recovery, affidandosi al service provider. Alla Pubblica Amministrazione residuerà pianificazione del Disaster Recovery Plan, per l’attivazione degli strumenti messi a disposizione dal provider.

Il DRaaS si basa sulla **replica e sull'hosting dei server in un site del PSN diverso rispetto all'ubicazione primaria**. Il cliente ha perciò in mano uno strumento da attivare nel momento in cui, nell’esecuzione del proprio Disaster Recovery Plan, decide di attivare l’altra ubicazione per rispondere ad un evento disastroso.

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 **Disaster Recovery as a Service 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 e a beneficio di tutte le parti coinvolte.

LA SICUREZZA DEL TUO SERVIZIO CLOUD E' UNA RESPONSABILITÀ 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, Transparency 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 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 sviluppate e gestite da parte del cliente.
RUNTIMES	Moduli eseguibili messi a disposizione dal 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

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 della Pubblica Amministrazione Cliente **identificare le componenti del proprio workload di servizio che intende far ridondare su altra componente geografica messa a disposizione** di PSN**.** Si ribadisce che rimane a carico del cliente **determinare le modalità di utilizzo dello strumento di DR**, attraverso la predisposizione ed il test periodico di specifiche **strategie di Disaster Recovery.**

Responsabilità PSN (CSP)

Nell'ambito dei servizi DRaaS, PSN mette a disposizione uno strumento di gestione attraverso il quale poter ridondare il proprio servizio in Datacenter diverso**.** Il suo utilizzo rimane di esclusiva responsabilità del cliente**.** E' infatti responsabilità del CSC determinare le modalità di utilizzo di tale strumento attraverso la definizione di apposite strategie di Disaster Recovery, le quali dovranno essere inoltre manutenute e testate,

SERVICE LAYERS

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

Legenda Responsabilità

= P.A.
= PSN
= N/A
= Condivisa

1 – Descrizione Servizi

2 – Metodologia

3 – Aree di responsabilità

4 - Riepilogo

Shared Security Responsibility Model

Matrice di sintesi

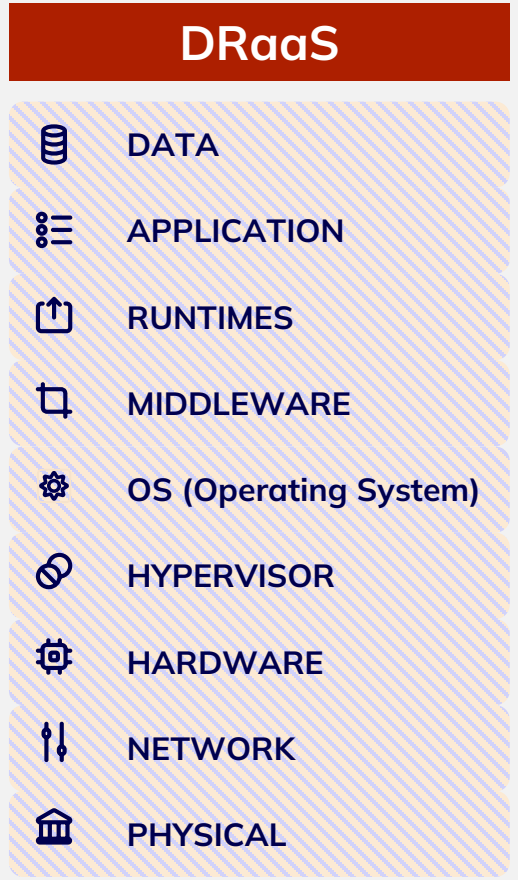
A riepilogo degli ambiti di responsabilità descritti all'interno documento, è possibile riassumere che per i servizi **DRaaS** la sicurezza del servizio è suddivisa secondo le seguenti aree di responsabilità:

Responsabilità Pubblica Amministrazione (CSC)

Il servizio DRaaS è acquistabile esclusivamente come integrazione ad un altro servizio erogato da PSN. Pertanto, **ad eccezione di quanto specificato nel dominio BCR**, assume le stesse responsabilità indicate nella Matrice di Responsabilità del servizio al quale viene associato.

Responsabilità PSN (CSP)

Il servizio DRaaS è acquistabile esclusivamente come integrazione ad un altro servizio erogato da PSN. Pertanto, **ad eccezione di quanto specificato nel dominio BCR**, assume le stesse responsabilità indicate nella Matrice di Responsabilità del servizio al quale viene associato.



Polo Strategico Nazionale

Cloud sicuro per l'Italia digitale.

www.polostrategiconazionale.it