asm vigevano lomellina s.p.a.

CLOUD SECURITY POLICY

SISTEMA DI GESTIONE INTEGRATO

Codice documento	**CLOUSP01**
Versione	**1.5 del 30/08/2024**
Livello di confidenzialità	**PUBBLICO**

	Preparato	*Controllato*	*Approvato*
	Resp. Funzione Fabio Tonelli	**RGQ** Francesca Graziotin	**RDSGI** Fabio Tonelli
Firma			
Data	30/08/2024	30/08/2024	30/08/2024

Registro delle modifiche

Data	Versione	Prodotta da	Descrizione delle modifiche
02/04/2020	1.0	Fabio Tonelli	Versione iniziale del documento
02/04/2021	1.1	Fabio Tonelli	Aggiornamento documento
05/12/2022	1.2	Fabio Tonelli	Aggiornamento documento
04/10/2023	1.3	Fabio Tonelli	Aggiornamento documento
14/11/2023	1.4	Fabio Tonelli	Modificata etichetta documento
30/08/2024	1.5	Fabio Tonelli	Aggiornamento documento

Indice

Scopo, ambito di applicazione e interessati

Lo scopo di questo documento è garantire una gestione corretta e sicura dell'infrastruttura dell'ambiente cloud.

Questo documento è applicato all'intero ambito ISMS (Information Security Management System), a tutta l'infrastruttura e ai dati dell'ambiente cloud, e alla relativa documentazione.

Gli utenti di questo documento sono dipendenti e collaboratori ASM Vigevano che si occupano dell'infrastruttura cloud.

Riferimenti normativi

- ISO/IEC 27001 standard, clauses 05.37, 08.06, 08.15.01, 08.15.02, 08.17, 08.22, 08.32.03
- ISO/IEC 27017 standard, clauses 6.1.1, 9.4.4, 12.1.2, 12.1.3, 12.4.1, 12.4.4, 13.1.3, 18.1.2 e controlli CLD.6.3.1, CLD.8.1.5, CLD.9.5.1, CLD.9.5.2, CLD.12.1.5, CLD.12.4.5, and CLD.13.1.4
- ISO/IEC 27018 standard, clauses 12.4.1 and A.9.2

Gestione sicura dell'ambiente cloud

Responsabilità della gestione del cloud

Il Business Continuity Manager è responsabile della gestione e del controllo dell'infrastruttura, delle piattaforme e dei servizi resi disponibili negli ambienti cloud,

Il Security Manager è responsabile della definizione delle funzionalità di sicurezza e del livello dei servizi previsti per tutti i servizi cloud, indipendentemente dal fatto che tali servizi siano forniti internamente o esternalizzati, i requisiti devono essere documentati con i fornitori di servizi.

È pertanto necessario che il Responsabile IT:

1. separi le responsabilità operative tra quelle di ASM Vigevano e quelle dei clienti del servizio cloud in merito all'ambiente cloud (infrastruttura, applicazioni, servizi e dati)
2. identifichi in collaborazione con il Security Manager i requisiti per qualsiasi programma di utilità da utilizzare all'interno dell'ambiente cloud
3. garantisca la disponibilità della documentazione necessaria, su sito web o documentazione elettronica inviata via email, ai clienti del servizio cloud in modo che possano adempiere correttamente alle loro responsabilità

Responsabilità della protezione del cloud

Il Security Manager è responsabile della protezione dell'infrastruttura, delle piattaforme e dei servizi resi disponibili negli ambienti cloud da accessi non autorizzati e perdita di integrità o disponibilità.

È pertanto necessario che:

- Il Security Manager separi le responsabilità di sicurezza tra quelle di ASM Vigevano. e quelle dei clienti del servizio cloud in merito all'ambiente cloud (infrastruttura, applicazioni, servizi e dati)
- Il Security Manager attivi le protezioni adeguate all'accesso e all'uso dei programmi di utilità all'interno dell'ambiente cloud tramite le tecnologie descritte nel documento "Specification of Information System Requirements"
- Il Responsabile IT garantisce la disponibilità degli ambienti cloud tramite le tecnologie seguenti:
  - linea di collegamento ad Internet con SLA 100% di disponibilità e duplicata
  - linee di alimentazione duplicate in data center con doppia fonte di alimentazione, doppio gruppo elettrogeno, doppia batteria di UPS, doppia linea di collegamento con l'armadio rack
  - doppio router, ciascuno attestato a ciascuna delle linee di collegamento ad Internet, con doppio alimentatore
  - sui router è configurato il protocollo BGP e BGPv6 verso Internet che garantisce il cambio automatico tra linea primaria e secondaria
  - sui router è configurato il protocollo OSPF verso i firewall interni per garantire il cambio automatico di router in caso di guasto ad uno dei due apparati
  - doppio switch con collegamenti ridondati con ciascun apparato
  - doppio server di virtualizzazione con collegamenti ridondati a switch e storage, doppio alimentatore, doppio disco in RAID-1 per il boot del sistema operativo, ventole duplicate
  - storage con doppio alimentatore per ciascun chassis, doppio gruppo di ventole per ciascun chassis, doppio collegamento dei controller con i chassis aggiuntivi, doppio controller attivo/attivo.
  - sistema di monitoraggio dei sistemi su server dedicato
  - sistema di monitoraggio ambientale
  - sistema di condizionamento ridondato
  - sistema di estinzione incendio a gas a saturazione
  - controlli accessi con badge per l'apertura porte di accesso al data center e log degli accessi centralizzati nel sistema di gestione del data center
  - backup su NAS locale e remota su sito di disaster recovery
  - replica delle macchine virtuali su sito di disaster recovery
  - possibilità di trasferire gli indirizzi pubblici mediante configurazione manuale del BGP dal data center primario al data center di disaster recovery
- Il Security Manager garantisca la segregazione dell'ambiente cloud tra gli ambienti dei clienti del servizio cloud e tra l'ambiente dei clienti del servizio cloud e l'ambiente di gestione interno di ASM Vigevano mediante:
  - VLAN dedicata per ogni servizio e per l'ambiente di gestione interno
- Il Security Manager garantisce l'applicazione di hardening practices dei componenti fisici e logici (ad es. unità di archiviazione, macchine virtuali, protocolli di servizio, ecc.) dell'infrastruttura cloud, in particolare:
  - cambio delle password di default dei componenti hardware
  - disattivazione dei servizi non essenziali sui server, router e switch
  - tutti i servizi vengono posti dietro firewall
  - tutti i servizi esposti su Internet vengono posti in DMZ definite su VLAN dedicate

- vulnerability assessment su ogni servizio con servizio leader di mercato e risoluzione di ogni segnalazione di livello superiore al 2 o in alternativa applicazione di un workaround

Per quanto riguarda la protezione dei dati negli ambienti cloud, il Security Manager è responsabile di assicurare che i dati necessari per le procedure di test dei clienti cloud, in particolare le informazioni di identificazione personale (PII), siano gestiti attraverso adeguate misure tecniche e organizzative proporzionali al rischio connesso a tali procedure di test.
Il Security Manager è responsabile di garantire l'efficacia dei controlli di sicurezza implementati per proteggere gli ambienti cloud e le informazioni ivi archiviate ed elaborate, mediante il monitoraggio e la verifica regolari dei controlli implementati.

Monitoraggio del cloud

Sulla base dei risultati della valutazione del rischio, dei requisiti legali e normativi e delle condizioni generali per i servizi cloud il Security Manager decide quali log verranno conservati sull'accesso e sull'uso degli ambienti cloud, sull'allocazione e sull'utilizzo delle risorse e sulle modifiche alle informazioni personali identificabili (PII) e deciderà i tempi di retention.

I log devono essere conservati per tutti gli amministratori e gli operatori che svolgono attività in ambienti cloud.

Il Responsabile IT è responsabile di garantire la corretta sincronizzazione dell'orologio tra gli orologi dei servizi cloud e gli orologi dei server cloud di ASM Vigevano tramite protocollo NTP con i server di riferimento ufficiali Italiani.

Il CSM è responsabile del monitoraggio giornaliero degli errori segnalati automaticamente, nonché degli errori segnalati dagli utenti, al fine di analizzare il motivo per cui si sono verificati gli errori e intraprendere le azioni correttive appropriate.

Il Security Manager è responsabile della revisione regolare dei log al fine di monitorare le attività degli utenti, degli amministratori e degli operatori cloud. La revisione viene condotta agli intervalli prescritti dal RDSGI, che determina e seleziona i log da rivedere e come verrà registrata la revisione. Il RDSGI deve essere informato sui risultati della revisione.

Il Security Manager è responsabile della revisione periodica dei log relativi alle Informazioni di identificazione personale (PII) al fine di identificare comportamenti insoliti rispetto alla gestione delle PII. La revisione viene condotta agli intervalli prescritti dal RDSGI, che determina e seleziona i record da rivedere e come verrà registrata la revisione. Il RDSGI deve essere informato sui risultati della revisione.

Il Capacity Manager è responsabile della revisione periodica dei log e dei database al fine di monitorare le risorse allocate e utilizzate da ciascun cliente del servizio cloud. La revisione viene condotta ad intervallo mensile. Il Responsabile IT deve essere informato sui risultati della revisione.

Il Change Manager deve informare con 30 giorni di anticipo il CSM circa modifiche che interessino i servizi cloud dei clienti, in particolare:

- descrizione sommaria delle modifiche
- data, ora e durata dell'eventuale disservizio
- descrizione tecnica delle modifiche

il CSM è responsabile di comunicare ai clienti con almeno 10 giorni di anticipo e ricordandoglielo due giorni prima ed il giorno stesso dell'intervento, assicurandosi che questi ricevano la comunicazione, la data, l'ora, la durata del disservizio e la descrizione sommaria delle modifiche. In caso di impedimento o impossibilità di comunicare con il cliente il CSM deve informare il RDSGI, che dovrà decidere come procedere, ed il Change Manager.

Rimozione degli asset dei clienti dal servizio cloud

Il Responsabile IT è responsabile di informare i clienti del servizio cloud mediante le condizioni generali di servizio o clausole nel contratto di servizio in merito alle modalità per la restituzione e la rimozione degli asset (dati, macchine virtuali, ecc.) del cliente al termine dell'accordo per l'uso di un servizio cloud.

Le modalità di restituzione e rimozione delle attività devono essere documentate nell'accordo di servizio e dovrebbe essere eseguito in modo tempestivo, dimensione dei dati permettendo. Le disposizioni devono specificare anche gli asset che verranno restituiti e quelli che verranno cancellati.

Il CSM è responsabile di ottemperare queste disposizioni, o in alternativa deve comunicare al cliente come procedere in autonomia al download dei dati.

Selezione fornitori di servizi cloud

I fornitori di servizi cloud che impattano sui servizi cloud erogati ai clienti di ASM o che trattano dati personali devono essere presenti sul Marketplace di ACN.

Gestione delle registrazioni conservate sulla base di questo documento

Nome registro	***Luogo di archiviazione***	***Persona responsabile della archiviazione***	***Diritti di inserimento/modifica***
Livello di servizio previsto per i servizi cloud	CMDB	Responsabile IT	Solo il Responsabile IT può inserire o modificare questi documenti.
Funzionalità di sicurezza	Archivio Documenti Progettuali	Responsabile IT	Solo il Responsabile IT può inserire o modificare questi documenti.
Registri delle revisioni dei log	CMDB	RDSGI	Le revisioni possono essere inserite da Responsabile IT, Capacity Manager e Security Manager. Solo il RDSGI può modificarle o cancellarle.

Validità e gestione dei documenti

Questo documento è valido a partire dalla data di emissione.

Il proprietario di questo documento è il RDSGI, che deve controllare e, se necessario, fare aggiornare il documento almeno una volta all'anno.

Nel valutare l'efficacia e l'adeguatezza di questo documento, devono essere considerati i seguenti criteri:

- numero di incidenti di sicurezza relativi all'infrastruttura dell'ambiente cloud
- numero di incidenti dovuti a responsabilità poco chiare per il funzionamento dell'infrastruttura dell'ambiente cloud

Le versioni precedenti di questa policy devono essere conservate per un periodo di 5 anni, se non diversamente specificato dai requisiti legali o contrattuali.