"POLITICA DI SICUREZZA DELLE INFORMAZIONI NELL'EROGAZIONE DI SERVIZI CLOUD"

5	Paola Massolo	16/07/2024	Michele Zunino	16/07/2024
REV. VIGENTE	COMPILATO DA RSGI (FIRMA)	DATA COMPILAZIONE	APPROVATO DA DIR (FIRMA)	DATA APPROVAZIONE PER EMISSIONE

ELENCO DELLE REVISIONI		
REV	DATA	DESCRIZIONE DELLE REVISIONI
0	31/10/2016	Prima emissione
1	14/02/2017	Seconda emissione
2	01/09/2018	Completa revisione per integrazione con norme ISO 27017 e ISO 27018
3	07/02/2023	Revisione per introduzione Sistema di Gestione Integrato e integrazione norma ISO27035
4	02/04/2024	Introduzione SSRM
5	16/07/2024	Implementazione SSRM

INDICE

1.0 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche quali conseguenza della politica generale del Sistema di Gestione Integrato (PolGenSGI r0) definita dalla Direzione di Netalia relativamente al campo di applicazione definito relativo al servizio Cloud per la protezione dei dati globali, inclusi i dati personali applicando le best practices presenti nel settore normativo (ISO 27017, ISO 27018, ISO27035).

La seguente politica, e le politiche aziendali derivanti da essa, viene rivista in caso di cambiamenti significativi o almeno una volta all'anno in occasione del riesame della Direzione eventualmente confermandone la validità.

2. DOCUMENTI DI RIFERIMENTO

UNI EN ISO 27001:2014 - Sistemi di gestione per la sicurezza delle informazioni – Requisiti

UNI EN ISO 27017:2015 - Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud

UNI EN ISO 27018:2014 - Codice di pratica per la protezione delle informazioni personali (PII) in cloud pubblici che agiscono come processori PII

UNI EN ISO 27035-1: 2016 – Information security incident management

GDPR (Reg. UE 679/2016 e legislazione nazionale – D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i.)

Codice etico

Lettera applicazione SGSI ai Dipendenti e Collaboratori

3. POLITICA DI SICUREZZA DI GESTIONE SERVIZIO CLOUD

3.1 POLITICA DI SICUREZZA DELLA GESTIONE DEL SERVIZIO CLOUD

Tulle le informazioni gestite da Netalia riedono nella infrastruttura logica che compone il cloud.

Tali informazioni possono essere riconducibili ai seguenti elementi:

a) Elementi strutturali del cloud e loro configurazioni
b) Configurazione degli ambienti logici assegnati ai clienti
c) Informazioni e dati applicativi dei clienti stessi.

I dipendenti e collaboratori di Netalia hanno accesso esclusivamente alle informazioni al punto a) e b), mentre non hanno possibilità alcuna di accesso agli elementi di tipo c) se non dietro esplica richiesta e permesso da parte del cliente per motivi di assistenza, manutenzione o aggiornamento.

L'infrastruttura fisica nel suo complesso è protetta da firewall perimetrali che abilitano solo le porte strettamente necessarie ai servizi erogati.

L'accesso di amministrazione relativo a quanto descritto al precedente punto a) è possibile solo per i tecnici Netalia con connessioni protette site-to-site o client-to-site SSL VPN.

L'accesso di amministrazione per i clienti relativo a quanto descritto nel punto b) è disponibile con connessioni protette e cifrate via HTTPS oppure in modalità client-to-site SSL VPN per i clienti che lo richiedono esplicitamente.

La sicurezza (riservatezza, integrità, disponibilità) dei dati viene garantita

- dall'esterno l'azienda (es.: cyber attacchi)
- dall'interno all'azienda (es.: danni e azioni accidentali da parte del personale tecnico)

dai seguenti punti 3.1.1 – 3.1.3, sotto il controllo del sistemista responsabile.

Tutte le informazioni applicative ed i relativi elaborati sono esclusiva responsabilità del cliente per quanto attiene il loro contenuto e il loro aggiornamento e rimangono sotto il controllo del Operational Manager esclusivamente per quanto attiene l'integrità e la disponibilità.

Per consentire ai clienti di definire, eseguire e sfruttare l'ambiente di sicurezza fornito da NETALIA, sono stati sviluppati programmi di controlli di sicurezza che implementa best practice di protezione della privacy e dati di livello globale. Queste procedure di sicurezza e controllo sono convalidate in modo indipendente tramite valutazioni di terze parti.
Il programma di controlli si basa sulla verifica, la dimostrazione e il monitoraggio:

- verifica che i servizi e le strutture di propria competenza prevedano un ambiente di controllo che funzioni in maniera efficace, attraverso policy, processi e attività di controllo, che comprende le persone, i processi e la tecnologia necessari a definire e a gestire un ambiente che supporti l'efficacia operativa del framework di controllo implementando i controlli specifici applicabili al cloud computing identificati dai più importanti organismi di settore, costantemente monitorati per identificare ed applicare pratiche all'avanguardia;
- dimostrazione della compliance di Netalia per contribuire a verificare la compliance del cliente rispetto ai requisiti governativi e di settore e per fornire informazioni sulle policy, sui processi e sui controlli definiti e gestiti;
- viene effettuato il monitoraggio per mantenere la compliance a standard globali e best practice, adottando innumerevoli requisiti nell'ambito dei controlli di sicurezza.

3.1.1 Programmi di controllo

Netalia identifica e definisce i programmi di controllo in base a certificazioni / attestazioni, leggi, regolamenti e privacy e allineamenti/quadri.

Le Certificazioni / attestazioni sono rilasciate da un organismo di audit di terza parte.

Le Leggi / regolamenti / privacy e allineamenti / quadri sono specifici in base al settore o alla funzione svolta.

Gli ambienti sotto sottoposti a continue verifiche, mentre l'infrastruttura e i servizi sono approvati per l'utilizzo in base a diversi standard di compliance.

Tra questi:

ISO 27001: è uno standard di sicurezza globale ampiamente adottato che definisce i requisiti per i sistemi di gestione della sicurezza delle informazioni. Garantisce un approccio sistematico alla gestione delle informazioni dell'azienda e del cliente in base a valutazioni periodiche del rischio;

ISO 27017: fornisce orientamenti sugli aspetti di sicurezza informatica che riguardano il cloud computing e raccomandazioni riguardo all'implementazione di controlli sulla sicurezza delle informazioni specifici per il cloud, che integrano le linee guida delle norme ISO 27002 e ISO 27001. Questo codice di condotta fornisce indicazioni sull'implementazione dei controlli per la sicurezza delle informazioni che riguardano specificamente i fornitori di servizi cloud;

ISO 27018: è un codice internazionale delle best practice incentrato sulla protezione dei dati personali nel cloud. Si basa sullo standard ISO 27002 relativo alla sicurezza delle informazioni e fornisce indicazioni per l'implementazione dei controlli ISO 27002 che si applicano alle informazioni di carattere personale nel cloud pubblico;

ISO 27035: è un codice internazionale delle best practice incentrato sulla gestione degli incidenti. Fornisce le linee guida per l'implementazione di procedure e controlli al fine di creare un approccio strutturato per la gestione degli incidenti.

La conformità di Netalia documenta che Netalia dispone di un sistema di controlli rivolto specificatamente a proteggere la privacy dei contenuti affidati dai clienti.

3.1.2 Sicurezza dei dati rispetto ai guasti hardware

L'infrastruttura logica abilitante, che consente la gestione delle informazioni descritte ai punti a), b) e c) è realizzata secondo modelli funzionali di alta affidabilità e ridondanza, che garantiscono copia e replica dei dati secondo politiche specifiche, su apparati distinti ed indipendenti.

3.1.3 Sicurezza del sistema rispetto all'intrusione

Le infrastrutture fisiche relative al cloud Netalia sono ospitate in ambienti fisici segregati ed indipendenti (cage) all'interno di un data center. L'accesso al data center ed alla cage sono gestiti da un sistema da una prima autenticazione visiva e da un controllo accessi con badge,

La lista degli utenti autorizzati all'accesso è comunicata dal Operational Manager Netalia al gestore del data center ed aggiornata quando necessario.

Il gestore del data center è dotato di certificazione ISO 27001.

3.1.4 Sicurezza dei dati rispetto al data center

I dati gestiti da Netalia possono essere replicati su infrastrutture fisiche distinte, in data center indipendenti in zone geografiche diverse.

3.1.5 Sicurezza al contorno

Al personale è fatto divieto:

a) Mantenere le sessioni di accesso alla infrastruttura aperte durante la loro assenza
b) Conservare in qualunque forma scritta (es. salvato su file, su browser, scritto su foglio) le proprie credenziali di accesso alla infrastruttura fisica, fatta eccezione per la password di superuser che è nota al sistemista responsabile e conservata in busta sigillata dal Operational Manager

3.1.6 Sicurezza del Sistema rispetto a Malware

Il software installato in piattaforma è unicamente software di base (Linux, Apache, Tomcat, Windows, etc.) scaricato da sorgenti autenticate e con controllo di digest. Solo il sistemista responsabile ha le autorizzazioni per installare nuovo software.

3.2 GESTIONE DEI DATI

I dati tecnologici dei clienti Netalia possono essere divisi in due categorie:

- Dati di Piattaforma
- Dati Applicativi

Netalia ha adottato Il Modello di responsabilità condivisa, che è un paradigma di sicurezza che definisce ruoli e responsabilità e garantisce trasparenza tra i clienti e il provider di servizi cloud.

La piattaforma di erogazione servizi cloud di Netalia è predisposta per l'erogazione di servizi di tipo IaaS e PaaS, ognuno con diversi livelli di responsabilità. Per il dettaglio sulle funzionalità, modalità di erogazione del servizio, e sulle caratteristiche trasversali di qualità, sicurezza, privacy e continuità operativa del servizio, si rimanda al Catalogo dei Servizi.

I clienti dovrebbero valutare attentamente i servizi che scelgono in quanto le loro responsabilità varieranno in funzione dei servizi usati, dell'integrazione di quei servizi nel loro ambiente IT e delle leggi e normative applicabili.

IaaS

Per quanto riguarda il servizio IaaS, Netalia applica i controlli di seguito indicati:

- gestione e mantenimento dell'infrastruttura (fisico e infrastruttura cloud)
- attività di patching infrastrutturale (fisico e infrastruttura cloud)
- attività di configurazione infrastrutturale (fisico e infrastruttura cloud)
- formazione dei propri dipendenti.

Le restanti componenti (e la loro gestione) sono responsabilità del Cliente, inclusa la formazione dei dipendenti del Cliente.

PaaS

Per quanto riguarda il servizio PaaS la responsabilità di Netalia in questo caso prevede, oltre alle già dette componenti del servizio IaaS, anche le componenti di:

- sistema operativo
- middleware
- runtime

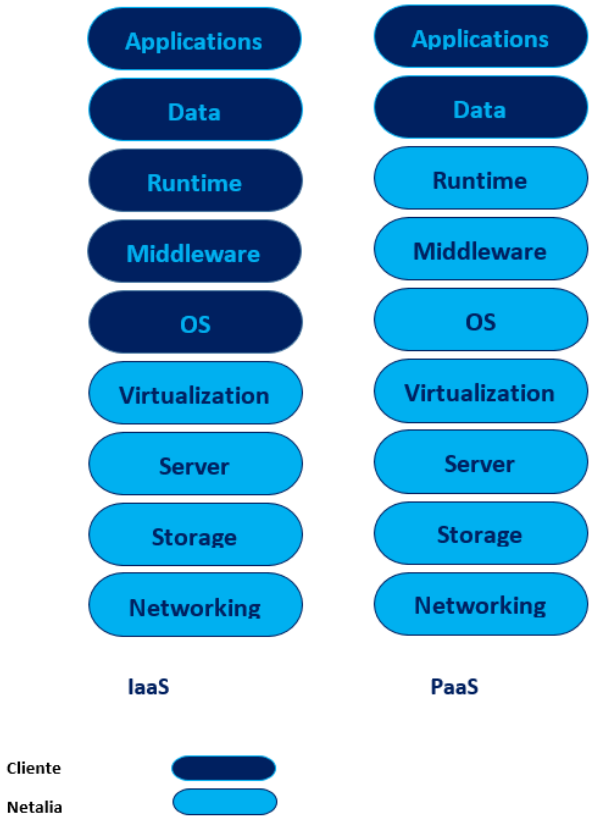
Restano di responsabilità del Cliente gli strati relativi a dati e applicazioni, nonché la loro gestione, e la formazione dei dipendenti del Cliente.

Inoltre, per tutti i tipi di servizio cloud fruito, il cliente ha la proprietà di dati e identità. L'utente del servizio cloud è responsabile della protezione dei dati e delle identità, delle risorse locali e dei componenti cloud che si controllano, che variano in base al tipo di servizio scelto.

Indipendentemente dal tipo di distribuzione, il cliente mantiene sempre le responsabilità seguenti riguardo i propri:

- endpoint
- accessi al servizio.

SSRM - Modello di responsabilità condivisa



3.2.1 Sicurezza dei contenuti

Netalia presta molta attenzione alla privacy dei suoi clienti. Il cliente resta sempre proprietario dei suoi contenuti mantenendo, tra l'altro, la possibilità di crittografarli, spostarli e gestirne la conservazione. Netalia fornisce strumenti che permettono di crittografare facilmente i dati in transito e inattivi, per garantire che solo gli utenti autorizzati possano accedervi.

Tali strumenti forniscono al cliente il controllo di cui necessità per essere conforme alle leggi e ai regolamenti (in ambito europeo) in materia di privacy. La struttura della nostra infrastruttura permette al cliente di mantenere il completo controllo sulla posizione geografica fisica in cui i dati sono ubicati, aiutandolo a soddisfare i requisiti in materia di posizione fisica dei dati.

Netalia non divulga i contenuti del cliente, salvo laddove sia richiesto dalla legislazione vigente o da ordinanze legali vincolanti emesse da un'autorità pubblica. Qualora Netalia fosse obbligata a divulgare i contenuti, verrà inviata una notifica preventiva al cliente per essere informato.

I data center di Netalia sono ubicati in Italia, per cui eseguire fisicamente lo storage dei dati è sempre sotto il controllo del cliente, il che semplifica la compliance ai requisiti territoriali e di posizione fisica dei dati.

3.2.2 Contenuti dei dati di Piattaforma
Possono essere raggruppati in 3 macro categorie.

3.2.2.1 Risorse assegnate al Cliente
Fanno parte di questa categoria le informazioni relative alle risorse definite nel contratto stipulato con Netalia ovvero:

- vCPU
- RAM
- storage
- networks
- IP pubblici
- eventuali licenze SW

3.2.2.2 Dati di accesso
Completata l'attivazione dell'ambiente del cliente (VPC) vengono fornite, al riferimento tecnico segnalato, le credenziali di accesso temporanee, con l'indicazione di cambiarle prima di procedere a qualsiasi attività.
Per questo motivo, nessun operatore Netalia, ha accesso all'ambiente e quindi ai dati sensibili interni alle VM (Virtual Machine) o agli applicativi del cliente.

3.2.2.3 Dati di log
Il personale tecnico Netalia può accedere ai log relativi all'andamento dei VPC dei vari clienti al solo scopo di monitorare il corretto funzionamento degli stessi e di conseguenza per analizzare e risolvere eventuali anomalie.
Trattandosi di log quali metriche VMware e utilizzo risorse, non riguardano dati sensibili dei clienti.

3.2.3 Gestione dei Dati Applicativi
Netalia non ha alcun accesso ai dati applicativi dei Clienti in quanto interni ad ogni singolo VPC (Virtual Private Cloud).
Netalia ha solo visibilità sul numero e tipologia di VM (Virtual Machine) che ogni cliente crea, siano esse attive o spente, senza aver modo di accedere ai dati in esse contenuti.

3.2.4 Continuità operativa
L'infrastruttura prevede un elevato livello di disponibilità con il continuo controllo della capacità; i sistemi sono progettati per tollerare errori hardware o di sistema con un impatto minimo per il cliente.

Il disaster recovery è il processo di preparazione per affrontare e risolvere una situazione grave dove si intende qualsiasi evento che abbia un impatto negativo sulla continuità operativa; il cloud di Netalia supporta diverse architetture di Disaster recovery.

3.3 REMOTE-SMART WORKING

Il remote-smart working è applicabile da contratto, ad eccezione di alcune mansioni dove è necessaria la presenza in ufficio.

È possibile accedere da postazioni remote, tramite password personale attraverso una SSL VPN.

3.4 CESSAZIONE DEL RAPPORTO DI LAVORO DEL PERSONALE NETALIA E/O DEI COLLABORATORI

Anche alla cessazione dell'attività, il dipendente o il collaboratore è tenuto alla riservatezza relativamente alle informazioni acquisite durante il rapporto di lavoro come definito dal contratto, dal codice (di comportamento) etico e Lettera applicazione SGSI ai Dipendenti e collaboratori.

3.5 CONTROLLI

I seguenti controlli sono effettuati periodicamente a campione:

1. Controlli sulla visibilità dei dati di piattaforma da parte di ciascun operatore
2. Controlli sul fatto che la password di ciascun operatore non sia scritta (accesso "a memoria")
3. Controlli sulle politiche del firewalling (revisione delle regole dei firewall)
4. Controllo del software installato nel sistema
5. Controllo dei log
6. Controllo a campione delle caratteristiche delle password (es. visionare la digitazione di un simbolo, o di una maiuscola o di un numero a richiesta del verificatore).
7. Verifica dei backup e della conservazione dello storico secondo policy.