POLITICA DI SICUREZZA DELLE INFORMAZIONI

NELLA GESTIONE DEI SERVIZI CLOUD

Infoteam P.IVA 01538680685
Viale Pindaro, 14 - 65127 Pescara (PE)

SOMMARIO

1 CLASSIFICAZIONE E REVISIONI DOCUMENTO

CLASSIFICAZIONE RISERVATEZZA DOCUMENTO						
Riservato		**Interno**		**Pubblico**		**x**
STATO REVISIONE						
Rev. N°	**Data**	**Motivo della revisione**	**Elaborata**	**Verificata**	**Approvata**	
1	25/07/2023	Emissione	RSGI	RCS	DIR	

2 INTRODUZIONE

La presente politica sintetizza l'impegno, espressamente dichiarato dall'organizzazione, a soddisfare i requisiti delle norme UNI EN ISO 27001:2022, UNI EN ISO 27017:2015, UNI EN ISO 27018:2019, GDPR (Reg. UE 679/2016 e legislazione nazionale – D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i.) e a integrazione della Politica generale del sistema di gestione per la sicurezza delle informazioni SGI-DOC-52-01, nell'ambito della progettazione, sviluppo, manutenzione evolutiva, erogazione e supporto per infrastrutture informatiche, applicativi e servizi cloud erogati in modalità Saas (software as a service), servizi di consulenza per la compliance normativa e servizi tecnici di assistenza e sicurezza informatica.

3 SCOPO

Il presente documento definisce, in coordinazione con la politica generale SGI-DOC-52-01, emanata dalla Direzione di Infoteam, i criteri direttivi generali relativi ai servizi cloud erogati. ciò al fine della protezione dei dati trattati e conservati in essi, inclusi quelli personali.
I criteri ivi sanciti derivano dalle best practices di cui agli standard di riferimento (ISO 27017:2015 e ISO 27018:2019).

4 POLITICA APPLICATA

4.1 Generalità

Le informazioni generate tramite i servizi cloud risiedono nell'infrastruttura logica che compone i servizi SaaS (infrastruttura IaaS, sistema operativo, middleware, applicativo e database).
Tali informazioni possono essere riconducibili alle seguenti tipologie:

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 Infoteam hanno accesso esclusivamente alle informazioni di cui al punto a) e b), mentre non hanno possibilità alcuna di accesso agli elementi di tipo c) se non dietro esplicita autorizzazione da parte del cliente per motivi di assistenza, manutenzione o aggiornamento.

L'accesso alle informazioni di cui ai precedenti punti a) e b), per l'esecuzione di operazioni amministrative, è possibile esclusivamente per i tecnici Infoteam (da intendersi come sviluppatori e sistemisti) tramite connessioni protette e cifrate (SSH / SSL).
L'accesso alle informazioni di cui al punto c) è possibile, ove previsto dalle relative condizioni contrattuali, per i soli tecnici di Infoteam e sempre con connessioni protette e cifrate.
La sicurezza (riservatezza, integrità, disponibilità) dei dati viene garantita con riferimento tanto alle minacce esterne (es: cyberattacchi) quanto alle minacce interne (es: dipendente infedele).
La responsabilità relativamente ai contenuti dei dati inseriti nei servizi cloud erogati, così come a tutte le attività riconducibili agli account dei clienti, è interamente in carico ai clienti finali, incaricati di utilizzare i servizi SaaS offerti adottando tutte le misure più idonee ai fini della sicurezza, della protezione e del salvataggio dei propri account e dei propri contenuti.
Infoteam si impegna, per ciascun servizio cloud, a garantire la sicurezza dell'ambiente operativo (sistema operativo, middleware etc…), dell'applicativo e del database e dunque della riservatezza, integrità e disponibilità dei dati.
A tal fine, sono state previste e predisposte pratiche e procedure di sicurezza. Esse sono convalidate in modo indipendente tramite valutazioni di terze parti. Inoltre, le stesse sono finalizzate a garantire la continua verifica della postura di sicurezza nonchè il monitoraggio degli eventi e dei risultati, il tutto in modo documentato e pertanto dimostrabile.

4.1.1 Programmi di controllo

Infoteam identifica e definisce i programmi di controllo necessari in base a certificazioni, attestazioni, leggi e regolamenti.
Le Certificazioni / attestazioni sono rilasciate da un organismo di audit di terza parte.

Leggi e regolamenti sono specifici in base al settore o alla funzione svolta.
L'ambiente cloud è sottoposto a continue verifiche per garantire la suddetta compliance, alla luce della quale l'infrastruttura ed i servizi sono approvati per l'utilizzo.
Tra i principali standard presi in considerazione per la compliance e la predisposizione dei programmi di controllo, vi sono:
ISO 27001:2022 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 27017:2015 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 27018:2019 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.
La compliance di Infoteam dimostra la disponibilità di un sistema di controlli rivolto specificatamente a proteggere la privacy dei contenuti affidati dai clienti.

4.1.2 Sicurezza dei dati rispetto ai guasti hardware

L'infrastruttura logica che consente la gestione delle informazioni descritte ai punti a), b) e c) è realizzata secondo modelli funzionali di alta affidabilità e ridondanza su apparati distinti ed indipendenti, che garantiscono copia e replica dei dati secondo politiche specifiche.
Ciò è reso possibile grazie alla scelta di sub-fornitori di datacenter cloud certificati ISO 27001 ed in grado dunque di dimostrare l'affidabilità e compliance delle rispettive infrastrutture ICT, tutte egualmente dotati di elevati standard di sicurezza e ridondanza.

4.1.3 Sicurezza del sistema rispetto all'intrusione

Le infrastrutture fisiche utilizzate per l'hosting dei servizi cloud erogati da Infoteam appartengono ai sub-fornitori – certificati ISO 27001 – scelti in base ai requisiti di certificazione, affidabilità, performance e sicurezza.
Tali infrastrutture rispondono ai criteri di sicurezza fisica di cui alla ISO 27001 e pertanto

garantiscono l'adozione delle misure necessarie a proteggere gli ambienti dall'intrusione, così come le misure atte a separare le reti, i sistemi ed i dati dei diversi tenant che fanno uso dell'infrastruttura.
I tecnici di Infoteam non accedono ai data center, riservato solo ai tecnici dei fornitori cloud, debitamente autorizzati.

4.1.4 Sicurezza dei dati

I dati gestiti da Infoteam per conto dei clienti possono essere replicati su infrastrutture fisiche distinte, in datacenter indipendenti e geograficamente diversi.
Ciò a garanzia di ridondanza e tempestiva ripresa dei servizi in caso di eventuali interruzioni.

4.1.5 Sicurezza delle operazioni

Al personale interno, con accesso ai servizi cloud per ragioni di assistenza/manutenzione/amministrazione, è fatto divieto:

- di mantenere le sessioni di accesso alla infrastruttura aperte durante la loro assenza
- di conservare in qualunque forma (es. su file, su browser, scritto su foglio) le credenziali di accesso alla infrastruttura al di fuori del password manager aziendale

4.1.6 Sicurezza del Sistema rispetto al Malware

I software installati sui sistemi cloud sono unicamente quelli serventi agli applicativi (es.: nginx, apache etc…), scaricati da sorgenti autenticate ed ufficiali previo controllo della corrispondenza fra pacchetto disponibile e pacchetto scaricato (tramite hash).
I sistemisti Infoteam sono gli unici autorizzati ad effettuare tali installazioni in sicurezza.
Periodicamente viene verificata l'eventuale presenza di malware od altre vulnerabilità tramite il processo di Vulnerability Assessment.

4.2 Gestione dei Dati

I dati digitali dei clienti Infoteam possono essere divisi in due categorie:

- Dati di Piattaforma
- Dati Applicativi

4.2.1 Sicurezza dei contenuti

Infoteam presta estrema attenzione alla privacy dei propri clienti. Il cliente resta sempre proprietario dei suoi contenuti mantenendo, tra l'altro, la possibilità di crittografarli, spostarli e gestirne la conservazione.
Infoteam non divulga i contenuti del cliente, salvo laddove sia richiesto dalla legislazione vigente o da ordinanze legali vincolanti emesse da un'autorità pubblica.
I datacenter dei fornitori cloud utilizzati da Infoteam sono ubicati in Italia, con ciò consentendo la compliance alle normative in tema privacy e a quelle di cybersecurity (es: il perimetro di sicurezza nazionale cibernetica).

4.2.2 Tipologie di dati e relativa disciplina

4.2.2.1 Risorse assegnate al Cliente

Fanno parte di questa categoria le informazioni relative alle risorse definite nel contratto stipulato fra Infoteam ed il Cliente, e dunque le caratteristiche tecniche che compongono il servizio, quali:

- Ip
- Cpu
- Memoria
- Spazio disco
- Etc…

4.2.2.2 Dati di accesso

Gli operatori tecnici (sistemisti e sviluppatori) di Infoteam hanno accesso all'ambiente cloud per ragioni amministrative o di manutenzione/assistenza e conseguentemente ai dati personali e sensibili interni alle virtual machines o ai database del cliente, come definito nel contratto e nelle nomine secondo GDPR.
In merito a tale accesso, esso è controllato e regolamentato.
In particolare:

- Le credenziali di accesso devono essere periodicamente cambiate e fare riferimento ad utenze nominative
- Le credenziali devono essere conservate su Passbolt
- Esclusivamente gli utenti autorizzati possono accedere alle risorse con le suddette credenziali, e solamente per ragioni di servizio ed in base alle proprie specifiche competenze.

4.2.2.3 Dati di log

I servizi cloud generano numerose tipologie di log, essenziali tanto per ragioni di operatività/performance quanto per ragioni di sicurezza (log dei webserver, log di sistema e così via).
Il personale tecnico di Infoteam può accedere ai log delle diverse istanze cloud al solo scopo di monitorare il corretto funzionamento delle stesse e di conseguenza per analizzare e risolvere eventuali anomalie.

4.2.3 Gestione dei Dati Applicativi

I tecnici Infoteam, per ragioni di manutenzione e supporto e secondo quanto strettamente previsto nei contratti, possono avere accesso ai dati generati/trattati attraverso gli applicativi sviluppati ed in particolare contenuti nei database.
Tale accesso avviene esclusivamente per ragioni di rilascio (aggiornamenti e bugfix), supporto e manutenzione evolutiva. I dati non vengono in alcun modo analizzati, utilizzati ed estrapolati.

4.2.4 Continuità operativa

L'infrastruttura cloud 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.
In particolare:

- Le risorse ed i relativi carichi sono costantemente monitorati tramite i pannelli di amministrazione forniti dai cloud providers di cui ci si serve e tramite Zabbix
- La capacità, tanto computazionale quanto di storage, è controllata ed aumentata laddove necessario
- I dati, in particolare i database, sono soggetti a backup quotidiano, e ciò consentirebbe di ripristinare il servizio in caso di fault od altro disastro che colpisse l'infrastruttura cloud
- Ci si affida a diversi cloud providers, in modo da poter ripristinare i servizi presso organizzazioni ed aree geografiche diverse.

4.3 Cessazione del rapporto di lavoro del personale dipendente e/o collaboratori di Infoteam

Alla cessazione dell'attività, il dipendente o il collaboratore è tenuto alla riservatezza relativamente alle informazioni acquisite durante il rapporto di lavoro, così come da impegno sottoscritto in fase di assunzione ed onboarding.

4.4 Controlli

I seguenti controlli sono effettuati periodicamente:

- Controlli sulla visibilità dei dati di piattaforma da parte di ciascun operatore
- Controllo sul corretto utilizzo del password manager centralizzato (Passbolt)
- Controlli sulle politiche di firewalling delle virtual machines
- Controllo del software installato nei sistemi
- Controllo dei log
- Verifica degli esiti dei backup.