Documento informativo sulla Sicurezza delle Informazioni per i servizi Cloud

1. INTRODUZIONE

Il presente documento, redatto in coerenza con i principi della norma ISO/IEC 27001 e con le linee guida della ISO/IEC 27017, ha lo scopo di fornire ai clienti una descrizione delle principali misure tecniche e organizzative adottate da SYSTEM LINE S.r.l. per la protezione delle informazioni nell'ambito dell'erogazione dei servizi cloud.

I servizi erogati da SYSTEM LINE S.r.l. si basano sull'utilizzo di infrastrutture e piattaforme cloud fornite da terze parti, che vengono configurate, gestite e integrate nell'ambito di servizi gestiti, al fine di fornire al cliente un ambiente operativo sicuro e coerente con le proprie esigenze.

SYSTEM LINE S.r.l. non si limita alla fornitura o rivendita di servizi cloud, ma progetta le architetture, configura gli ambienti, gestisce le identità e gli accessi, implementa misure di sicurezza, monitora i sistemi e interviene operativamente nella gestione dei servizi.

Il modello adottato si basa su una responsabilità condivisa tra il fornitore cloud, SYSTEM LINE S.r.l. e il cliente, nella quale:

- il fornitore cloud è responsabile della sicurezza dell'infrastruttura sottostante;
- SYSTEM LINE S.r.l. è responsabile della configurazione, gestione e sicurezza operativa degli ambienti cloud;
- il cliente mantiene la responsabilità sui dati trattati, sulle finalità di utilizzo e sulla definizione dei requisiti di sicurezza.

Il cliente si interfaccia con SYSTEM LINE S.r.l. quale referente tecnico e operativo per la gestione dei servizi, delegando le attività di configurazione, gestione e sicurezza degli ambienti cloud, sulla base delle proprie esigenze e istruzioni.

Il presente documento ha finalità informativa e consente ai clienti di comprendere le principali caratteristiche di sicurezza del servizio, la ripartizione delle responsabilità e le modalità di gestione dei rischi adottate da SYSTEM LINE S.r.l.

2. MODELLO DI RESPONSABILITÀ

Il modello di responsabilità in essere prevede il coinvolgimento di tre tipologie di soggetti: SYSTEM LINE S.r.l., il cloud provider e il cliente. A seconda del ruolo svolto nella progettazione, erogazione e fruizione del servizio cloud, si differenziano le rispettive responsabilità.

SYSTEM LINE S.r.l. eroga servizi cloud basati su infrastrutture e piattaforme fornite da terze parti, rispetto alle quali opera in qualità di cliente dei servizi cloud (CSC), assumendo al contempo il ruolo di fornitore di servizi gestiti (CSP) nei confronti del cliente finale.

SYSTEM LINE S.r.l. identifica e gestisce gli asset rilevanti per l'erogazione del servizio, al fine di garantirne un'adeguata protezione in relazione ai rischi associati. Il cliente mantiene la responsabilità in ordine alla correttezza, alla liceità e alla conformità dei dati trattati, nonché alla definizione delle esigenze, dei requisiti di sicurezza e delle politiche di utilizzo relative ai propri sistemi e informazioni.

SYSTEM LINE S.r.l. assicura che il personale coinvolto nell'erogazione del servizio sia adeguatamente formato e sensibilizzato in materia di sicurezza delle informazioni, attraverso attività periodiche di formazione e aggiornamento, al fine di garantire un comportamento coerente con le politiche di sicurezza adottate.

La sicurezza del servizio è gestita secondo un modello di responsabilità condivisa, nel quale:

- SYSTEM LINE S.r.l. è responsabile della progettazione, configurazione e gestione operativa degli ambienti cloud, inclusa la gestione delle identità e degli accessi, l'implementazione delle misure di sicurezza, il monitoraggio dei sistemi e la gestione degli incidenti, in conformità ai requisiti e alle istruzioni definite dal cliente;
- il fornitore IaaS/PaaS è responsabile della sicurezza dell'infrastruttura e dei servizi di base sottostanti;
- il cliente definisce i requisiti di sicurezza, le politiche di accesso e utilizzo, autorizza le configurazioni e mantiene la responsabilità sui dati trattati e sulle finalità del loro utilizzo.

Il cliente, pur non accedendo direttamente all'infrastruttura cloud, si interfaccia con SYSTEM LINE S.r.l. quale unico referente tecnico e operativo, delegando a quest'ultima le attività di configurazione, gestione e sicurezza degli ambienti cloud, sulla base delle istruzioni e delle esigenze definite.

SYSTEM LINE S.r.l. definisce e assegna ruoli e responsabilità in materia di sicurezza delle informazioni nell'ambito della propria organizzazione, al fine di garantire una gestione efficace e coordinata delle misure di sicurezza adottate.

SYSTEM LINE S.r.l., in qualità di fornitore del servizio, definisce e mantiene ruoli, competenze e responsabilità connesse ai processi di progettazione, configurazione e gestione degli ambienti cloud, applicando i principi di segregazione delle mansioni (*segregation of duties*), privilegio minimo (*least privilege*) e controllo duale *(dual control*), coerentemente con quanto stabilito dal provider.

Nell'ambito dei processi operativi, le attività sono strutturate in sequenze procedurali eseguite da soggetti differenti, al fine di evitare che il controllo dell'intero processo sia attribuito a un singolo individuo.

I diritti di accesso a locali, apparati, dati e funzionalità sono attribuiti al personale addetto esclusivamente nella misura necessaria all'espletamento delle mansioni assegnate, in applicazione del principio del privilegio minimo.

Il fornitori cloud autorizzati documentano e comunicano le proprie capacità di sicurezza, i ruoli e le responsabilità applicabili al servizio erogato, nonché le responsabilità che restano in capo al cliente; tali informazioni sono recepite e incorporate nei documenti interni, nella matrice di responsabilità e nei contratti.

La protezione degli hypervisor e dei componenti del piano di controllo dell'infrastruttura è responsabilità del fornitore IaaS/PaaS ed è oggetto di valutazione da parte di SYSTEM LINE S.r.l. sulla base della documentazione, delle certificazioni e delle attestazioni fornite dal provider, mentre la progettazione del servizio, mediante la configurazione e gestione degli ambienti cloud, assicura l'utilizzo di controlli di isolamento e segmentazione coerenti con le buone pratiche.

La ripartizione delle responsabilità sopra descritta rappresenta il modello generale adottato e può essere ulteriormente dettagliata nei rapporti contrattuali, negli accordi di servizio e nella documentazione tecnica di riferimento.

La seguente tabella rappresenta una sintesi della ripartizione delle responsabilità tra i soggetti coinvolti, fermo restando che le responsabilità operative di SYSTEM LINE S.r.l. sono esercitate sulla base delle istruzioni e dei requisiti definiti dal cliente e formalizzati nei rapporti contrattuali.

Ambito	Fornitore cloud	SYSTEM LINE S.r.l.	Cliente
Infrastruttura cloud (data center, hardware, virtualizzazione)	✓		
Sicurezza fisica e ambientale	✓		
Servizi di base (rete cloud, hypervisor, piattaforma)	✓		
Configurazione ambienti cloud		✓	Validazione requisiti
Architettura cloud		✓	Definizione esigenze
Gestione identità (creazione utenti, gruppi)		✓	Richiesta e autorizzazione

Definizione autorizzazioni e ruoli		✓ (implementazione)	✓ (definizione logica)
Autenticazione (MFA, policy accesso)		✓ (configurazione)	✓ (definizione requisiti)
Sicurezza configurativa (hardening, segmentazione)		✓	Approvazione / indirizzo
Monitoraggio e logging	✓ (strumenti)	✓ (gestione operativa)	Supervisione
Gestione incidenti		✓ (gestione tecnica)	Segnalazione / decisioni
Backup e replica dati	✓ (capability)	✓ (configurazione e gestione)	Definizione requisiti
Ripristino dati		✓ (esecuzione)	Richiesta
Crittografia (infrastrutturale)	✓		
Crittografia (configurazione/logica)		✓	Definizione esigenze
Dati (contenuti, correttezza, liceità)			✓
Classificazione dati		Supporto	✓
Conformità normativa		Supporto tecnico	✓

3. Gestione degli accessi e delle identità

L'accesso ai servizi cloud è consentito esclusivamente agli utenti autorizzati. La gestione delle identità e dei relativi diritti di accesso è effettuata da SYSTEM LINE S.r.l., sulla base delle richieste e delle autorizzazioni fornite dal cliente, mediante funzionalità dedicate messe a disposizione dall'ambiente cloud.

L'assegnazione dei diritti di accesso avviene sulla base di ruoli definiti, al fine di garantire che ciascun utente disponga esclusivamente delle autorizzazioni necessarie allo svolgimento delle proprie attività.

Sulla base dell'analisi del rischio e dei requisiti definiti dal cliente, SYSTEM LINE S.r.l. implementa meccanismi di autenticazione coerenti con il livello di rischio conseguente. Per gli utenti con privilegi amministrativi è prevista l'attivazione dell'autenticazione a più fattori.

Le credenziali sono gestite in modo da garantirne la riservatezza e non sono accessibili in chiaro.

All'attivazione del servizio, SYSTEM LINE S.r.l. provvede alla creazione delle utenze necessarie sulla base delle indicazioni fornite dal cliente; le credenziali possono essere modificate dagli utenti autorizzati secondo le modalità previste dal sistema.

Al termine della procedura di registrazione, il cliente ottiene l'assegnazione delle credenziali di accesso (nome utente e password), delle quali è responsabile sotto il profilo della custodia e del corretto utilizzo, anche in relazione alle attività svolte tramite tali credenziali.

Il cliente si impegna a:

a) comunicare tempestivamente a SYSTEM LINE S.r.l. qualsiasi utilizzo non autorizzato delle credenziali o violazione delle regole di sicurezza;

b) assicurare che gli utenti autorizzati effettuino il logout al termine delle sessioni.

SYSTEM LINE S.r.l. non può essere ritenuta responsabile per eventuali danni derivanti da un uso improprio delle credenziali imputabile al cliente o agli utenti da esso autorizzati.

Il cliente è consapevole che l'accesso al servizio avviene sulla base delle credenziali assegnate e che è responsabile della loro corretta gestione interna, inclusa la comunicazione agli utenti autorizzati e la revoca degli accessi non più necessari.

Ogni operazione effettuata mediante credenziali valide è attribuita all'utente cui le credenziali sono associate. SYSTEM LINE S.r.l. può utilizzare le registrazioni dei sistemi informatici come evidenza delle operazioni effettuate.

I servizi prevedono funzionalità per la gestione del ciclo di vita delle utenze, inclusa la creazione, modifica, sospensione e cancellazione, effettuate da SYSTEM LINE S.r.l. su richiesta o autorizzazione del cliente.

4. LOGGING E MONITORAGGIO

Le risorse e i servizi sono organizzati secondo criteri di segregazione logica, al fine di garantire l'isolamento tra ambienti, utenti e componenti del sistema.

I sistemi cloud utilizzati mettono a disposizione funzionalità di registrazione degli eventi e di monitoraggio, che vengono configurate e gestite da SYSTEM LINE S.r.l. in funzione delle esigenze del servizio e dei requisiti definiti dal cliente.

I log sono protetti da accessi non autorizzati e alterazioni e sono conservati per un periodo coerente con le esigenze operative, di sicurezza e di conformità normativa.

L'accesso alle informazioni di log è limitato ai soggetti autorizzati.

SYSTEM LINE S.r.l. configura e utilizza le funzionalità di logging e monitoraggio messe a disposizione dall'infrastruttura cloud utilizzata, distinguendo tra:

- logging infrastrutturale, gestito dal provider;
- logging operativo e di sicurezza, configurato e monitorato da SYSTEM LINE S.r.l.

I sistemi in essere permettono la registrazione, la memorizzazione e l'analisi dei log, in particolare con riferimento a:

- accessi al sistema;
- disponibilità dei sistemi;
- anomalie operative;
- performance delle risorse;
- operazioni amministrative;
- attività privilegiate;
- eventi di sicurezza.

SYSTEM LINE S.r.l. svolge attività di monitoraggio continuo degli eventi rilevanti ai fini della sicurezza e della continuità operativa, al fine di identificare anomalie, comportamenti sospetti o condizioni di rischio.

I clienti sono informati, per il tramite di SYSTEM LINE S.r.l., in merito agli eventi rilevanti che possono compromettere la sicurezza o la disponibilità del servizio, secondo modalità coerenti con gli accordi contrattuali e con i processi di gestione degli incidenti.

I sistemi adottano meccanismi di sincronizzazione temporale basati su fonti affidabili, al fine di garantire la coerenza degli eventi registrati e supportare le attività di monitoraggio, analisi e gestione degli incidenti.

5. BACKUP E CONTINUITÀ OPERATIVA

Le risorse utilizzate per l'erogazione del servizio sono monitorate e gestite al fine di garantire adeguati livelli di capacità e prestazioni, anche in funzione della scalabilità delle soluzioni cloud adottate e per prevenire incidenti di sicurezza riconducibili a carenze di risorse, quali indisponibilità, degradi di servizio o malfunzionamenti dei controlli di sicurezza.

Qualora siano necessarie attività straordinarie di adeguamento della capacità che possano influire temporaneamente sulle prestazioni o sulla disponibilità, i clienti sono informati mediante i canali ufficiali con indicazione della finestra operativa.

Sono effettuati backup periodici dei dati, con frequenza e modalità definite in funzione delle configurazioni del servizio e dei requisiti concordati con il cliente. I backup sono conservati su infrastrutture separate rispetto ai sistemi primari.

I backup sono protetti mediante misure di sicurezza adeguate al fine di prevenire accessi non autorizzati, alterazioni o perdite di dati.

Per quanto riguarda i servizi gestiti, la progettazione, configurazione ed esecuzione dei backup sono effettuate da SYSTEM LINE S.r.l., sulla base delle esigenze e dei parametri definiti dal cliente, assicurandone il corretto funzionamento mediante controlli e verifiche periodiche.

SYSTEM LINE S.r.l. garantisce la possibilità di configurare politiche di conservazione dei dati coerenti con le esigenze del cliente (ad esempio backup incrementali giornalieri, backup settimanali o retention differenziate), nonché la possibilità di effettuare ripristini selettivi secondo le modalità concordate.

I sistemi di backup prevedono meccanismi di notifica in caso di anomalie o malfunzionamenti.

Il cliente definisce i requisiti di backup e continuità operativa in funzione delle proprie esigenze e può richiedere operazioni di ripristino secondo le modalità previste.

L'accesso diretto ai sistemi di backup non è generalmente previsto; eventuali richieste di esportazione o copia dei dati sono gestite da SYSTEM LINE S.r.l. secondo quanto stabilito nei rapporti contrattuali.

SYSTEM LINE S.r.l. implementa, ove previsto dalle configurazioni del servizio, meccanismi di replica e protezione dei dati, inclusa la possibilità di utilizzare ambienti distinti per finalità di resilienza e continuità operativa.

Le misure di continuità operativa sono definite in funzione delle caratteristiche del servizio e possono includere piani di ripristino, obiettivi di recupero (RTO) e di perdita dati (RPO), nonché attività di verifica periodica, nei limiti delle configurazioni adottate e degli accordi contrattuali.

Attività	Provider Cloud	SYSTEM LINE S.r.l.	Cliente
Progettazione ed esecuzione dei backup	Mette a disposizione funzionalità e infrastrutture per il backup e la protezione dei dati.	Progetta e configura i backup dei servizi gestiti ed esegue le attività operative, sulla base dei requisiti e dei parametri definiti dal cliente.	Definisce i requisiti di backup (frequenza, retention, criticità) in funzione delle proprie esigenze.
Controlli, verifiche e test dei backup	Garantisce l'affidabilità delle funzionalità di backup a livello infrastrutturale.	Effettua controlli, verifiche e test periodici per assicurare l'affidabilità dei backup, nei limiti delle configurazioni adottate.	Valuta i risultati rispetto alle proprie esigenze di continuità operativa.
Conservazione dei dati (retention)	Fornisce capacità di conservazione secondo le caratteristiche del servizio cloud.	Configura e gestisce la conservazione dei backup secondo i parametri concordati.	Definisce e approva i parametri di conservazione dei dati.
Ripristino dei dati (restore)	Fornisce le funzionalità tecniche di ripristino.	Esegue le operazioni di ripristino secondo le modalità tecniche previste.	Richiede il ripristino e ne definisce priorità e ambito.
Protezione dei backup	Garantisce misure di sicurezza a livello infrastrutturale (es. protezione dello storage, resilienza).	Implementa misure tecniche e organizzative per proteggere i backup da accessi non autorizzati, alterazioni o perdite.	Definisce eventuali requisiti specifici di sicurezza in funzione dei dati trattati.
Copertura delle componenti incluse nei backup	Mette a disposizione strumenti e servizi che consentono il backup delle componenti supportate.	Include nei backup le componenti del servizio secondo le configurazioni adottate (dati, configurazioni, componenti operative).	Verifica che le componenti coperte siano coerenti con le proprie esigenze.
Gestione anomalie e notifiche	Fornisce funzionalità di monitoraggio e segnalazione a livello infrastrutturale.	Attiva sistemi di monitoraggio e notifica in caso di anomalie o malfunzionamenti dei backup.	Riceve le notifiche e valuta eventuali azioni conseguenti.

Replica e resilienza dei dati	Fornisce meccanismi di replica geografica e resilienza dell'infrastruttura.	Implementa, ove previsto, configurazioni di replica e protezione dei dati in ambienti distinti.	Definisce il livello di resilienza richiesto in funzione delle proprie esigenze.
Accesso ai backup	Non consente accesso diretto ai backup a livello infrastrutturale, se non tramite funzionalità del servizio.	Non prevede accesso diretto; gestisce eventuali richieste di copia o esportazione secondo quanto stabilito contrattualmente.	Può richiedere copia o esportazione dei dati secondo le modalità contrattuali.
Politiche di backup del cliente	Fornisce strumenti che possono essere utilizzati per politiche di backup personalizzate.	Supporta, ove richiesto, la definizione di politiche di backup integrate con il servizio.	Definisce eventuali politiche interne aggiuntive (es. copie locali, esportazioni).

6. Classificazione delle informazioni

Le informazioni gestite nell'ambito dei servizi sono soggette, ove applicabile, a meccanismi di classificazione ed etichettatura coerenti con il sistema di sicurezza adottato, al fine di garantirne una gestione e protezione adeguata lungo il ciclo di vita.

SYSTEM LINE S.r.l. adotta criteri e strumenti per la classificazione delle informazioni nell'ambito dei propri sistemi e processi interni, al fine di garantire un'adeguata protezione in funzione della sensibilità delle informazioni trattate.

Per quanto riguarda i dati trattati nell'ambito dei servizi cloud, la classificazione delle informazioni è di responsabilità del cliente, che definisce il livello di protezione necessario in relazione alle proprie esigenze e al contesto di utilizzo.

SYSTEM LINE S.r.l., sulla base delle indicazioni fornite dal cliente, configura e gestisce i sistemi in modo da supportare l'applicazione dei livelli di classificazione definiti, anche mediante l'implementazione di controlli coerenti con tali livelli, quali, a titolo esemplificativo, la gestione degli accessi, l'applicazione di misure di protezione dei dati e la configurazione delle politiche di sicurezza.

I servizi possono prevedere funzionalità che consentono al cliente di classificare o etichettare le informazioni e le risorse associate, attivabili in funzione delle specifiche configurazioni adottate.

7. ISOLAMENTO E SEGREGAZIONE IN AMBIENTI MULTI-TENANT

Il servizio è progettato per operare in ambienti multitenant e adotta meccanismi di segregazione logica al fine di garantire l'isolamento tra clienti, ambienti e componenti del sistema. L'isolamento è realizzato su più livelli, tenendo conto sia delle caratteristiche dell'infrastruttura cloud sottostante, sia delle configurazioni applicative e di sicurezza implementate.

In particolare:

- il fornitore cloud garantisce meccanismi di isolamento a livello infrastrutturale;
- SYSTEM LINE S.r.l. progetta, configura e gestisce i meccanismi di segregazione logica, assicurando la separazione tra ambienti, tenant, dati e risorse, in funzione delle esigenze del servizio e dei requisiti definiti dal cliente.

L'isolamento copre i livelli dati, applicazioni, sistemi operativi, storage e rete, mediante configurazioni del perimetro, segmentazione delle risorse, separazione degli spazi di archiviazione e definizione di ambiti di accesso (scoping) coerenti con il contesto di utilizzo.

Le attività di amministrazione interna di SYSTEM LINE S.r.l. sono mantenute separate dalle risorse utilizzate dai clienti, attraverso l'utilizzo di account dedicati, canali di gestione distinti e controlli di accesso indipendenti.

SYSTEM LINE S.r.l. applica inoltre il principio del minimo privilegio e adotta misure di controllo degli accessi e delle identità coerenti con i livelli di segregazione definiti, al fine di prevenire accessi non autorizzati o interferenze tra ambienti.

7. CRITTOGRAFIA

SYSTEM LINE S.r.l. adotta un approccio strutturato all'utilizzo della crittografia per la protezione dei dati, in coerenza con le proprie politiche di sicurezza.

I dati sono protetti in transito mediante l'utilizzo di protocolli sicuri (es. HTTPS/TLS) e, ove previsto, a riposo mediante meccanismi di cifratura dello storage messi a disposizione dall'infrastruttura cloud utilizzata.

SYSTEM LINE S.r.l. configura e gestisce l'utilizzo delle funzionalità crittografiche disponibili, in funzione delle esigenze del servizio e dei requisiti definiti dal cliente.

La gestione delle chiavi crittografiche a livello infrastrutturale è effettuata dal fornitore cloud, mentre SYSTEM LINE S.r.l. ne valuta le caratteristiche e ne governa l'utilizzo nell'ambito delle configurazioni adottate.

Il cliente può definire specifici requisiti in materia di protezione dei dati e crittografia, che vengono recepiti da SYSTEM LINE S.r.l. nella configurazione dei servizi, nei limiti delle funzionalità disponibili.

L'utilizzo della crittografia è disciplinato da criteri e policy interne che definiscono le modalità di applicazione in funzione dei rischi e della natura delle informazioni trattate.

8. RESTITUZIONE, RIMOZIONE E CANCELLAZIONE DEI DATI ALLA CESSAZIONE

Alla cessazione del rapporto contrattuale, il cliente può richiedere l'esportazione dei propri dati relativi al servizio in formati documentati, secondo le modalità previste dalla documentazione del servizio e dagli accordi contrattuali.

A seguito della richiesta del cliente e del completamento delle attività di esportazione, SYSTEM LINE S.r.l. procede alla disattivazione del tenant e alla rimozione degli asset del cliente dai sistemi applicativi di produzione.

L'organizzazione assicura che i periodi di conservazione dei dati definiti dal cliente siano implementati e rispettati nei sistemi applicativi di produzione, in coerenza con le configurazioni adottate.

Eventuali persistenze residue nei sistemi di backup, gestiti direttamente o tramite fornitori di infrastruttura cloud, sono limitate al tempo strettamente necessario per esigenze di continuità operativa e comunque non eccedono i cicli tecnici di retention; tali dati non sono accessibili né utilizzabili per finalità operative.

La cancellazione dei dati è effettuata mediante metodologie coerenti con le caratteristiche dell'infrastruttura cloud utilizzata e conformi alle buone pratiche di sicurezza delle informazioni, al fine di ridurre il rischio di accesso non autorizzato o recupero dei dati.

Il perimetro degli asset interessati comprende i dati del cliente del servizio cloud (contenuti applicativi, configurazioni del tenant e allegati), nonché i dati derivati dal servizio pertinenti al tenant del cliente, come descritto nella documentazione del servizio.

Le tempistiche e le fasi del processo (disattivazione, esportazione dati, rimozione da produzione, cancellazione da backup e archivi) sono definite in funzione delle configurazioni adottate e degli accordi contrattuali e possono essere oggetto di evidenze su richiesta.

9. GESTIONE DELLE VULNERABILITÀ

L'infrastruttura cloud utilizzata è soggetta a processi di gestione delle vulnerabilità da parte del fornitore cloud, che provvede alla gestione delle vulnerabilità a livello infrastrutturale secondo le proprie procedure e priorità.

SYSTEM LINE S.r.l., nell'ambito dei servizi gestiti, adotta un approccio strutturato alla gestione delle vulnerabilità relativo alle configurazioni, ai sistemi e ai componenti utilizzati per l'erogazione del servizio, al fine di ridurre i rischi per la sicurezza delle informazioni

In particolare, SYSTEM LINE S.r.l. applica criteri di configurazione sicura e hardening per le risorse e i componenti gestiti, assicurando che siano abilitati esclusivamente porte, protocolli e servizi

necessari e che siano implementate adeguate misure tecniche, quali, ove applicabile, protezioni antimalware, logging e monitoraggio.

Le attività di verifica della sicurezza possono includere, in funzione delle esigenze del servizio, delle richieste del cliente o di specifici obblighi normativi, l'esecuzione di Vulnerability Assessment e, ove applicabile, Penetration Test.

SYSTEM LINE S.r.l. tiene conto delle informazioni relative alle vulnerabilità fornite dal provider cloud e, ove necessario, adotta le opportune misure correttive a livello di configurazione e gestione operativa.

10. GESTIONE DELLE MODIFICHE

Le modifiche ai servizi sono gestite mediante un processo strutturato che prevede la classificazione delle modifiche, l'analisi degli impatti, la valutazione dei rischi, l'esecuzione di test, l'approvazione da parte delle funzioni competenti e la completa tracciabilità delle attività svolte.

Il processo di gestione delle modifiche considera anche gli impatti sui dati e sui servizi dei clienti, inclusi gli effetti su disponibilità, integrità e sicurezza delle informazioni trattate.

Le modifiche sono classificate in base alla loro criticità e tipologia (ordinaria, significativa, urgente) e sono gestite secondo livelli di controllo proporzionati al rischio.

SYSTEM LINE S.r.l. gestisce operativamente il processo di modifica, assicurando che le attività siano eseguite in conformità alle procedure definite e, ove necessario, sulla base delle autorizzazioni e delle indicazioni fornite dal cliente.

Le modifiche sono comunicate ai clienti secondo criteri proporzionati alla loro criticità. In particolare, le modifiche non urgenti con impatto significativo sono comunicate con un preavviso minimo di 10 giorni lavorativi, mentre le modifiche urgenti possono essere implementate senza preavviso, con successiva informazione al cliente.

L'organizzazione tiene conto delle modifiche introdotte dai fornitori di servizi cloud utilizzati per l'erogazione del servizio, valutandone gli impatti sugli ambienti gestiti e adottando le eventuali misure necessarie a livello di configurazione e gestione operativa.

SYSTEM LINE S.r.l. identifica le operazioni critiche la cui esecuzione, in caso di errore, può comportare danni non recuperabili agli asset trattati nel servizio, e disciplina tali operazioni mediante procedure formalizzate, approvate, tracciate e soggette a supervisione e controllo degli accessi.

A titolo esemplificativo, rientrano tra le operazioni critiche l'installazione, la modifica e la cancellazione di componenti virtualizzati e risorse (ad esempio server, reti e storage), le procedure di cessazione del servizio e le attività di backup e ripristino.

Su richiesta, SYSTEM LINE S.r.l. mette a disposizione dei clienti la documentazione di riferimento relativa a tali operazioni critiche, al fine di consentire una corretta valutazione dell'impatto e il coordinamento delle attività.

11. SVILUPPO SICURO

I servizi sono configurati, implementati e, ove applicabile, sviluppati secondo principi di sicurezza integrati nel ciclo di vita delle soluzioni adottate.

I requisiti di sicurezza sono definiti nelle fasi di progettazione e configurazione dei servizi e sono mantenuti lungo tutte le fasi del ciclo di vita.

SYSTEM LINE S.r.l. adotta linee guida e criteri di sicurezza per garantire la protezione delle informazioni e la resilienza dei servizi, sia nelle attività di configurazione e gestione degli ambienti cloud, sia, ove applicabile, nelle attività di sviluppo software.

Le attività di sviluppo, quando previste, sono disciplinate da linee guida e policy interne che definiscono i principi di sviluppo sicuro adottati.

Nell'ambito dei servizi gestiti, SYSTEM LINE S.r.l. applica inoltre configurazioni sicure e pratiche di hardening ai componenti utilizzati, al fine di ridurre la superficie di attacco e garantire un adeguato livello di sicurezza.

Ove richiesto dal cliente, SYSTEM LINE S.r.l. può fornire indicazioni relative alle configurazioni di sicurezza adottate, incluse le impostazioni raccomandate, i servizi abilitati e le misure tecniche disponibili, al fine di supportare l'adozione di configurazioni sicure.

12. GESTIONE DEI FORNITORI

SYSTEM LINE S.r.l. adotta criteri e principi per la selezione e gestione dei fornitori, al fine di garantire che i servizi erogati da terze parti siano coerenti con i requisiti di sicurezza delle informazioni e con le esigenze del servizio.

I requisiti di sicurezza applicabili ai fornitori sono definiti e formalizzati nell'ambito dei rapporti contrattuali.

I fornitori sono valutati sulla base di requisiti di sicurezza, affidabilità e conformità e sono oggetto di monitoraggio e riesame periodico. Ove applicabile, sono privilegiati fornitori in possesso di certificazioni riconosciute in materia di qualità e sicurezza delle informazioni.

Nel caso dei servizi cloud utilizzati per l'erogazione del servizio, i fornitori di infrastruttura rappresentano una componente essenziale della catena di fornitura. SYSTEM LINE S.r.l. valuta le caratteristiche di sicurezza dei servizi cloud utilizzati e integra le relative misure nell'ambito delle proprie configurazioni e dei controlli adottati.

Le modifiche rilevanti ai servizi forniti da terze parti sono valutate al fine di analizzarne l'impatto sulla sicurezza delle informazioni e sulla continuità del servizio.

Sono considerati i rischi derivanti dalla catena di fornitura ICT, inclusi eventuali fornitori indiretti.

I fornitori cloud sono considerati parte integrante della catena di fornitura e i relativi rischi sono gestiti in funzione dell'impatto sui servizi erogati, anche mediante attività di valutazione, monitoraggio e integrazione delle misure di sicurezza disponibili.

13. GESTIONE DEGLI INCIDENTI

SYSTEM LINE S.r.l. adotta procedure per la gestione degli incidenti di sicurezza delle informazioni, al fine di garantire una risposta tempestiva, efficace e coordinata agli eventi che possono compromettere la sicurezza, la disponibilità o l'integrità dei servizi.

Nell'ambito dei servizi gestiti, SYSTEM LINE S.r.l. svolge attività di monitoraggio e rilevazione degli eventi di sicurezza, al fine di individuare tempestivamente anomalie, comportamenti sospetti o incidenti.

Sono individuati ruoli e responsabilità per la gestione degli incidenti, che comprendono le attività di rilevazione, analisi, classificazione, gestione e risoluzione degli eventi.

Gli incidenti possono essere segnalati sia da sistemi automatici di monitoraggio, sia da parte degli utenti o del cliente, che è tenuto a comunicare tempestivamente eventuali eventi rilevanti riscontrati.

SYSTEM LINE S.r.l. gestisce operativamente gli incidenti relativi agli ambienti e alle configurazioni di propria competenza, coordinandosi con il cliente per la valutazione degli impatti e per l'adozione delle eventuali misure correttive.

Nel caso di incidenti riconducibili ai servizi cloud sottostanti, SYSTEM LINE S.r.l. si interfaccia con il fornitore cloud, monitorando l'evoluzione dell'evento e adottando le misure necessarie a livello di configurazione e gestione del servizio.

I clienti sono informati in merito agli incidenti che possono avere impatti sui servizi o sui dati trattati, secondo modalità coerenti con gli accordi contrattuali e con la gravità dell'evento.

Le evidenze relative agli incidenti sono raccolte, conservate e protette al fine di supportare le attività di analisi, miglioramento e, ove necessario, eventuali esigenze legali o forensi.

14. CONFORMITÀ NORMATIVA

SYSTEM LINE S.r.l. identifica e monitora i requisiti normativi e regolamentari applicabili alle proprie attività e ai servizi erogati, al fine di garantire un adeguato livello di conformità in materia di sicurezza delle informazioni.

Il cliente mantiene la responsabilità in ordine alla conformità dei dati trattati e delle finalità del trattamento, mentre SYSTEM LINE S.r.l., nell'ambito dei servizi gestiti, supporta l'implementazione delle misure tecniche e organizzative necessarie per la protezione delle informazioni, sulla base delle istruzioni e dei requisiti definiti dal cliente.

SYSTEM LINE S.r.l. può mantenere, ove applicabile, contatti con le autorità competenti in materia di sicurezza delle informazioni e protezione dei dati, limitatamente agli ambiti di propria competenza e in relazione ai servizi erogati.

L'organizzazione tiene conto dei requisiti normativi applicabili anche nella selezione e gestione dei fornitori cloud e nell'utilizzo dei servizi cloud, valutando gli aspetti relativi alla localizzazione dei dati, alle modalità di trattamento e alle misure di sicurezza adottate.

Sono tutelati i diritti di proprietà intellettuale relativi al software e sono rispettati i diritti di terzi.

I registri e le informazioni rilevanti sono protetti al fine di garantirne l'integrità e la disponibilità.

L'utilizzo della crittografia avviene in coerenza con i requisiti normativi applicabili e con le politiche di sicurezza adottate.

15. MIGLIORAMENTO CONTINUO

La sicurezza delle informazioni è oggetto di riesami periodici, anche da parte di soggetti indipendenti rispetto alle attività operative, al fine di verificarne l'efficacia e l'adeguatezza rispetto ai rischi e al contesto di riferimento.

SYSTEM LINE S.r.l. adotta un approccio di miglioramento continuo delle misure di sicurezza, basato sull'analisi delle evidenze raccolte nell'ambito delle attività operative, tra cui il monitoraggio dei sistemi, la gestione degli incidenti, la gestione delle vulnerabilità e l'evoluzione delle configurazioni dei servizi.

Le informazioni derivanti da tali attività sono utilizzate per identificare opportunità di miglioramento, aggiornare le configurazioni, rafforzare i controlli di sicurezza e adeguare le modalità di gestione dei servizi.

Il processo di miglioramento tiene conto dell'evoluzione tecnologica, dei rischi emergenti, delle modifiche ai servizi cloud utilizzati e dei requisiti normativi applicabili.

Ove necessario, le modifiche alle misure di sicurezza e alle configurazioni dei servizi sono implementate secondo processi controllati e coerenti con le procedure di gestione delle modifiche.

Michele Rocchini

General Manager - System Line Srl

SYSTEM LINE SRL
Sede: 50053 EMPOLI (FI)
Via 1° Maggio, 75
Tel. 0571.72329 - Fax 0571.74702
C.F. e P.IVA 03197970480