POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/03/2026	Luca Buran	Stefano Torricella

Indice

Scopo

La presente politica esprime e formalizza l'impegno del Top Management di Syscon Srl verso la protezione del patrimonio informativo aziendale. In qualità di documento quadro al vertice del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), essa costituisce il riferimento per istituire, attuare, mantenere e migliorare in modo continuativo il sistema stesso, con l'obiettivo di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito della progettazione, sviluppo e distribuzione di soluzioni software e servizi cloud, comprese le attività di installazione e manutenzione presso i clienti.

L'organizzazione riconosce che la sicurezza delle informazioni rappresenta un fattore strategico per la continuità del business e per il mantenimento della fiducia dei propri clienti — imprese e organizzazioni del settore pubblico — e si impegna a perseguire un livello di protezione proporzionato alla natura e alla criticità degli asset informativi trattati, nel rispetto dei requisiti normativi e contrattuali applicabili.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici di Syscon Srl presso la sede operativa di Via Como 5, 30027 San Donà di Piave (VE). Essa coinvolge tutto il personale dipendente, i collaboratori a contratto e le terze parti che accedono alle informazioni o ai sistemi aziendali, ivi inclusi i fornitori di servizi cloud critici. Sono escluse dall'ambito di applicazione le attività relative alla taratura di strumenti di misura e le lavorazioni su beni materiali del cliente, in quanto non pertinenti al contesto operativo dell'organizzazione.

Riferimenti normativi

- ISO/IEC 27001:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.

- **Sistema di gestione della sicurezza delle informazioni (SGSI)** : insieme di politiche, procedure, linee guida, risorse e attività associate, gestite collettivamente dall'organizzazione al fine di proteggere i propri asset informativi.
- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione delle conseguenze di un evento e della relativa probabilità di accadimento.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa a un sistema, servizio o rete, che indica una possibile violazione della politica di sicurezza o un fallimento dei controlli, oppure una situazione precedentemente sconosciuta che può avere rilevanza per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni, indesiderati o inattesi, che hanno una probabilità significativa di compromettere le attività operative e di minacciare la sicurezza delle informazioni.
- **Asset** : qualsiasi elemento che ha valore per l'organizzazione, incluse informazioni, software, hardware, servizi e persone.
- **Controllo** : misura che modifica il rischio, inclusi processi, politiche, dispositivi, pratiche o altre condizioni e azioni.

Ruoli e responsabilità

- **Datore di Lavoro** : approva la presente politica, alloca le risorse necessarie all'attuazione del SGSI e assicura l'allineamento degli obiettivi di sicurezza delle informazioni con la strategia aziendale.
- **Responsabile del sistema di gestione** : supervisiona l'implementazione e il mantenimento della politica, ne coordina la comunicazione agli stakeholder interni ed esterni e gestisce il riesame periodico del SGSI.
- **Resp. Tecnico** : assicura che le infrastrutture IT e i servizi cloud adottino i controlli tecnici coerenti con i principi espressi nella presente politica.
- **Full Stack Developer** : opera nel rispetto delle regole di sicurezza definite, trattando le informazioni in conformità alla loro classificazione durante le attività di sviluppo software.
- **System Integrator** : applica le misure di protezione degli asset informativi durante le attività di installazione, configurazione e manutenzione presso i clienti.
- **Resp. Commerciale** : integra i requisiti di sicurezza delle informazioni nella gestione delle relazioni con clienti e nella definizione degli accordi contrattuali.

Obiettivi di sicurezza delle informazioni

Syscon Srl persegue obiettivi di sicurezza delle informazioni coerenti con il proprio contesto di business, il profilo di rischio e gli indirizzi strategici del Top Management. L'organizzazione si impegna a:

- proteggere la riservatezza dei dati dei clienti, del codice sorgente proprietario e delle informazioni aziendali classificate, prevenendo accessi non autorizzati e divulgazioni indebite;
- garantire l'integrità delle soluzioni software sviluppate e dei dati gestiti attraverso i servizi cloud, assicurando che modifiche e trattamenti avvengano esclusivamente da parte di soggetti autorizzati e secondo processi controllati;
- mantenere la disponibilità dei sistemi informativi e dei servizi erogati ai clienti, riducendo i tempi di indisponibilità e assicurando la capacità di ripristino in caso di eventi avversi;
- adempiere ai requisiti normativi e contrattuali applicabili in materia di protezione dei dati e sicurezza delle informazioni, con particolare riguardo alla legislazione sulla privacy;
- promuovere la consapevolezza di tutto il personale in merito alle minacce alla sicurezza e alle responsabilità individuali, attraverso attività di formazione e sensibilizzazione pianificate;
- favorire il miglioramento continuo del SGSI mediante la misurazione delle prestazioni, il riesame della direzione e l'attuazione di azioni correttive derivanti da audit, incidenti e variazioni del contesto delle minacce.

Ciascun obiettivo è declinato in indicatori di prestazione misurabili, documentati nel programma di miglioramento e riesaminati periodicamente dalla direzione al fine di verificarne l'adeguatezza e il grado di raggiungimento.

Principi fondamentali di sicurezza delle informazioni

Approccio basato sul rischio

L'organizzazione adotta un approccio sistematico alla gestione del rischio quale fondamento per l'individuazione e l'attuazione dei controlli di sicurezza. Ogni decisione relativa al trattamento delle informazioni tiene conto della probabilità e dell'impatto delle minacce identificate, con soglie di accettabilità definite e trattamenti documentati nella valutazione del rischio aziendale. I rischi connessi alla sicurezza delle informazioni — dall'accesso non autorizzato ai sistemi alla compromissione degli ambienti di sviluppo — sono identificati, analizzati, trattati e monitorati secondo la metodologia descritta nella *PRO Procedura di gestione dei rischi* .

Responsabilità condivisa e consapevolezza

La protezione delle informazioni è responsabilità di ogni persona che opera per conto di Syscon Srl. Il Top Management promuove una cultura della sicurezza in cui ciascun membro del personale comprende il proprio ruolo nel preservare la riservatezza, l'integrità e la disponibilità dei dati, agisce in conformità alle politiche e procedure del SGSI, e partecipa alle attività di formazione e sensibilizzazione pianificate. Tale principio si estende ai collaboratori esterni e ai fornitori che accedono ai sistemi o alle informazioni aziendali, i quali sono tenuti al rispetto degli obblighi di riservatezza e delle regole d'uso definite dall'organizzazione.

Uso accettabile delle informazioni e delle risorse

Syscon Srl richiede che tutte le informazioni e le risorse associate — sistemi, reti, applicazioni, servizi cloud — siano utilizzate esclusivamente per finalità aziendali legittime e nel rispetto della classificazione assegnata. L'organizzazione identifica e documenta gli utenti autorizzati all'accesso alle informazioni, specificando per ciascuno i sistemi e le repository a cui è consentito l'accesso. Il trattamento delle informazioni classificate come Riservato, Limitato o Pubblico segue le regole definite nella *POL Politica di classificazione ed etichettatura delle informazioni* , e i dettagli operativi per l'uso quotidiano delle risorse IT sono disciplinati dalla *POL Politica di sicurezza operativa* .

Segnalazione degli eventi di sicurezza

L'organizzazione promuove una cultura della segnalazione tempestiva e senza ritorsioni di qualsiasi evento — osservato o sospetto — che possa indicare una violazione della sicurezza delle informazioni, un fallimento dei controlli o una situazione anomala. Ogni membro del personale è tenuto a comunicare immediatamente gli eventi di sicurezza attraverso i canali definiti dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* . Gli eventi segnalati sono registrati nel *MOD Registro degli incidenti di sicurezza delle informazioni* , classificati per gravità e gestiti attraverso un processo strutturato di contenimento, eradicazione e ripristino, con l'obiettivo di minimizzare l'impatto operativo e prevenire il ripetersi dell'evento.

Scrivania pulita e schermo protetto

L'organizzazione adotta il principio della scrivania pulita e dello schermo protetto per ridurre il rischio di accesso non autorizzato alle informazioni durante e al di fuori dell'orario di lavoro. I documenti contenenti informazioni classificate non devono essere lasciati incustoditi sulle postazioni di lavoro e vanno riposti in modo sicuro al termine dell'utilizzo. I dispositivi sono configurati con blocco automatico dello schermo dopo un periodo di inattività e richiedono l'autenticazione per la riattivazione. L'efficacia di tali misure è verificata attraverso ispezioni periodiche degli uffici condotte al di fuori dell'orario lavorativo. Le regole operative di dettaglio sono stabilite nella *POL Politica di sicurezza operativa* .

Protezione degli asset fuori sede

Syscon Srl riconosce che le informazioni aziendali possono essere esposte a rischi addizionali quando trattate al di fuori dei propri locali, in particolare durante le attività di lavoro da remoto e di manutenzione presso le sedi dei clienti. L'organizzazione si impegna pertanto a garantire un livello di protezione equivalente a quello applicato in sede, adottando misure proporzionate al valore e alla classificazione degli asset coinvolti.

Lavoro da remoto

L'accesso ai sistemi aziendali da posizioni esterne è consentito esclusivamente attraverso connessione VPN aziendale e desktop remoto, utilizzando gli strumenti messi a disposizione dall'organizzazione. L'installazione di strumenti di accesso remoto di tipo

permanente e non autorizzati è vietata. Lo smart working è praticabile solo se preventivamente concordato con l'azienda, se necessario per la gestione di emergenze, oppure se imposto da disposizioni di legge. Il personale in lavoro da remoto è tenuto a utilizzare reti domestiche protette e a mantenere attive le misure di protezione del dispositivo, inclusa la crittografia integrale del disco e il blocco automatico al termine dell'attività o in caso di assenza prolungata.

Attività presso i clienti

Il personale che opera presso le sedi dei clienti per installazioni, configurazioni o manutenzione custodisce le informazioni aziendali e i dati dei clienti con la medesima diligenza richiesta in sede, evitando l'esposizione di informazioni riservate in ambienti non controllati. I dispositivi utilizzati in trasferta sono dotati di crittografia e di funzionalità di cancellazione remota.

Smarrimento, furto o danneggiamento

Qualora un asset aziendale venga smarrito, rubato o danneggiato al di fuori della sede, il personale è tenuto a notificare senza indugio il **Resp. Tecnico** , attivando così le procedure di blocco remoto del dispositivo, revoca degli accessi e sostituzione delle credenziali compromesse. L'evento è gestito come incidente di sicurezza delle informazioni secondo quanto previsto dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Restituzione degli asset

Al termine di una trasferta, di un progetto o alla cessazione del rapporto di lavoro, ogni asset informativo affidato al personale è restituito all'organizzazione nella sua integrità, nel rispetto delle modalità definite dalla *PRO Procedura di configurazione, gestione e smaltimento degli asset* .

Archiviazione e aggiornamento

La presente politica è gestita come informazione documentata controllata all'interno del SGSI. Il **Responsabile del sistema di gestione** ne cura l'archiviazione, la distribuzione e l'aggiornamento secondo le modalità stabilite dalla *PRO Procedura di gestione delle informazioni documentate* . Il riesame avviene con cadenza annuale, o in occasione di cambiamenti significativi nel contesto organizzativo, tecnologico o nel panorama delle minacce, e i relativi esiti confluiscono nel riesame della direzione. Le versioni superate sono conservate per garantire la tracciabilità storica delle modifiche apportate.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni

- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione delle informazioni documentate
- MOD Registro degli incidenti di sicurezza delle informazioni