POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/03/2026	Davide Sangiovanni	Davide Sangiovanni

Indice

Scopo

La presente politica formalizza l'impegno della **Direzione Generale** di LANONE S.a.s verso la protezione degli asset informativi aziendali e costituisce il documento quadro al vertice del Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Attraverso di essa l'organizzazione definisce il riferimento strategico per istituire, attuare, mantenere e migliorare continuamente il SGSI, con l'obiettivo di preservare la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito dei servizi IT gestiti, della cybersecurity, delle soluzioni VoIP e cloud e dello sviluppo software erogati alla clientela B2B.

L'organizzazione riconosce che la sicurezza delle informazioni è un fattore abilitante per la fiducia dei propri clienti e per la sostenibilità del business; pertanto si impegna a bilanciare le esigenze di sviluppo economico e di creazione di valore con la tutela dei dati e delle infrastrutture, in coerenza con gli indirizzi strategici aziendali e con il contesto normativo applicabile.

Campo di applicazione

La politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici gestiti presso la sede operativa di Via Cremona 19, 26013 Crema (CR). Coinvolge tutto il personale dell'organizzazione — incluse le funzioni di helpdesk, sistemistica, sviluppo, cybersecurity, area commerciale e amministrazione — nonché collaboratori esterni e fornitori che accedono alle informazioni o ai sistemi aziendali nell'esecuzione delle proprie prestazioni.

Riferimenti normativi

- ISO/IEC 27001:2022
- Reg. (UE) 2016/679

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per cui l'informazione non è resa disponibile o divulgata a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza dell'informazione.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi.

- **Evento di sicurezza delle informazioni** : occorrenza identificata di uno stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza delle informazioni, un fallimento dei controlli o una situazione non conosciuta in precedenza che può essere rilevante per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Sistema di gestione della sicurezza delle informazioni (SGSI)** : la parte del sistema di gestione complessivo che, basandosi su un approccio risk-based, stabilisce, implementa, opera, monitora, riesamina, mantiene e migliora la sicurezza delle informazioni.

Ruoli e responsabilità

- **Direzione Generale** : approva la presente politica, assicura le risorse necessarie al SGSI e promuove la cultura della sicurezza delle informazioni in tutta l'organizzazione.
- **Responsabile del sistema di gestione** : sovrintende all'attuazione, al mantenimento e al miglioramento continuo del SGSI, coordina gli audit interni e gestisce la documentazione di sistema.
- **Qualità GDPR NIS2 ISO 27001** : coordina la gestione del rischio informativo, monitora l'efficacia dei controlli e supporta l'allineamento alla normativa sulla protezione dei dati.
- **Area Tecnica** : garantisce l'implementazione dei controlli tecnici di sicurezza sulle infrastrutture e sui servizi IT erogati.
- **Cybersecurity (EDR, Backup, SIEM, Audit, NIS2)** : gestisce le soluzioni di protezione degli endpoint, il monitoraggio degli eventi di sicurezza e la risposta agli incidenti.
- **Tutto il personale** : rispetta le regole definite dal SGSI, utilizza le risorse aziendali in modo conforme e segnala tempestivamente eventi o debolezze di sicurezza.

Obiettivi di sicurezza delle informazioni

LANONE S.a.s persegue i seguenti obiettivi strategici in materia di sicurezza delle informazioni:

- Garantire la protezione dei dati dei clienti B2B e delle infrastrutture gestite, preservandone riservatezza, integrità e disponibilità in coerenza con gli obblighi contrattuali e i livelli di servizio concordati.
- Mantenere un approccio sistematico alla valutazione e al trattamento dei rischi per la sicurezza delle informazioni, adottando tecnologie di settore — crittografia, backup ridondati, scansioni delle vulnerabilità, soluzioni EDR — proporzionate al livello di rischio individuato.
- Assicurare la conformità ai requisiti legali, regolamentari e contrattuali applicabili, con particolare riguardo alla protezione dei dati personali.

- Promuovere la consapevolezza di tutto il personale attraverso programmi di formazione continua sulle minacce e sulle buone pratiche di sicurezza.
- Garantire la continuità dei servizi IT critici erogati alla clientela mediante piani di continuità operativa e di ripristino di emergenza regolarmente testati.
- Favorire il miglioramento continuo del SGSI attraverso il monitoraggio degli indicatori di prestazione, la conduzione di audit interni e il riesame periodico da parte della Direzione.

Principi fondamentali di sicurezza delle informazioni

L'organizzazione fonda il proprio SGSI su un insieme di principi che guidano l'adozione dei controlli, le decisioni di investimento e il comportamento quotidiano di tutto il personale.

Approccio basato sul rischio

Ogni decisione in materia di sicurezza delle informazioni trae origine dalla valutazione dei rischi e delle opportunità identificati nel contesto organizzativo. L'organizzazione si impegna a identificare, analizzare e trattare i rischi con una metodologia strutturata, assegnando priorità di intervento sulla base della probabilità di accadimento e dell'impatto potenziale. Il trattamento dei rischi avviene attraverso misure tecniche, organizzative e contrattuali proporzionate al livello di rischio residuo accettabile.

Responsabilità condivisa

La sicurezza delle informazioni è responsabilità di ogni figura che opera all'interno dell'organizzazione o che interagisce con i suoi sistemi. La **Direzione Generale** assume l'impegno di rendere chiare le attribuzioni, di mettere a disposizione le risorse adeguate e di promuovere una cultura in cui la segnalazione di eventi e debolezze sia considerata un contributo positivo alla protezione degli asset.

Uso accettabile delle informazioni e delle risorse

L'organizzazione richiede che le informazioni e le risorse associate — hardware, software, connettività, supporti fisici e digitali — siano utilizzate esclusivamente per finalità professionali autorizzate, nel rispetto delle regole documentate nelle politiche e procedure del SGSI. Ogni risorsa è assegnata formalmente al personale mediante il *MOD Modulo di assegnazione dei beni* e il relativo registro degli utenti autorizzati, che ne specifica i sistemi, le repository e le informazioni accessibili. Il personale è tenuto a custodire con diligenza i beni ricevuti, a mantenerli in efficienza e a restituirli al termine del rapporto o su richiesta dell'organizzazione.

Scrivania pulita e schermo pulito

Al fine di prevenire accessi non autorizzati e la divulgazione di informazioni, l'organizzazione adotta il principio della scrivania pulita e dello schermo pulito. I documenti cartacei e i supporti di memorizzazione rimovibili contenenti informazioni riservate non possono essere lasciati incustoditi sulla postazione di lavoro al termine dell'attività o in

assenza del personale assegnatario. I dispositivi sono configurati con il blocco automatico dello schermo dopo cinque minuti di inattività, con richiesta delle credenziali di accesso al ripristino; lo spegnimento del display interviene a partire da cinque minuti in modalità batteria e da dieci minuti in modalità alimentazione. Tali impostazioni sono applicate centralmente e non possono essere disattivate dal personale.

Segnalazione degli eventi di sicurezza delle informazioni

L'organizzazione si impegna a fornire a tutto il personale, ai collaboratori e alle terze parti un meccanismo chiaro e accessibile per segnalare tempestivamente eventi di sicurezza osservati o sospetti. Qualunque situazione anomala — e-mail di phishing, attività sospette, debolezze nei sistemi, potenziali violazioni — è comunicata immediatamente al **Responsabile del sistema di gestione** tramite il canale di posta elettronica designato. La segnalazione tempestiva è un dovere di ciascun membro dell'organizzazione e non comporta conseguenze negative per il segnalante in buona fede. Ogni evento segnalato viene valutato, classificato e, se confermato, registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni* per garantire tracciabilità, analisi delle cause e miglioramento dei controlli.

Miglioramento continuo

L'organizzazione riconosce che il panorama delle minacce evolve costantemente; per questo si impegna a riesaminare periodicamente l'efficacia del SGSI, a tradurre le lezioni apprese dagli incidenti e dagli audit in azioni correttive concrete e a mantenere aggiornate le proprie politiche, procedure e competenze.

Protezione degli asset fuori sede

L'organizzazione si impegna a garantire la protezione degli asset informativi anche quando vengono utilizzati al di fuori dei propri locali, in particolare durante trasferte presso clienti, partecipazione a eventi di settore o consegne a fornitori. Sono considerati asset fuori sede notebook, dispositivi mobili, supporti di memorizzazione esterni e documenti cartacei trasportati per esigenze operative.

A tal fine l'organizzazione adotta i seguenti principi:

- **Custodia** : gli asset non sono mai lasciati incustoditi in veicoli, mezzi pubblici o aree comuni di strutture ricettive. Durante la trasferta il personale assegnatario li custodisce in un luogo chiuso a chiave o nella cassaforte della struttura ospitante, assumendone piena responsabilità.
- **Crittografia dei dispositivi** : tutti i notebook e le unità esterne assegnati al personale sono protetti con crittografia dell'intero disco, in modo che l'eventuale smarrimento o furto non comporti l'esposizione dei dati contenuti.
- **Trasporto** : l'asset resta in custodia personale diretta. Il trasporto in stiva di bagaglio aereo e l'invio tramite posta ordinaria non sono ammessi; per le consegne a fornitori o sedi distaccate l'organizzazione utilizza servizi di corriere tracciato.

- **Segnalazione di smarrimento, furto o danneggiamento** : il personale notifica immediatamente al **Responsabile del sistema di gestione** , e comunque entro ventiquattro ore dall'accadimento, qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le procedure di blocco remoto del dispositivo, revoca degli accessi e cambio delle credenziali; l'evento è registrato come incidente di sicurezza delle informazioni.
- **Restituzione** : al termine della trasferta, del progetto o del rapporto di lavoro l'asset è restituito all'organizzazione mediante il *MOD Modulo di assegnazione dei beni* .

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI. Il **Responsabile del sistema di gestione** ne assicura l'archiviazione nel sistema documentale aziendale, la distribuzione alle parti interessate e la revisione con cadenza annuale. Un riesame straordinario è avviato ogniqualvolta intervengano cambiamenti significativi nell'organizzazione, nella tecnologia o nel contesto delle minacce. Ogni revisione è approvata dalla **Direzione Generale** e comunicata a tutto il personale e alle terze parti interessate.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- POL Politica del sistema di gestione
- PRO Procedura di configurazione, gestione e smaltimento degli asset