POL Politica del sistema di gestione

Storia della versione

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

Indice

Scopo

LANONE S.a.s riconosce nella sicurezza delle informazioni un pilastro fondamentale della propria missione di erogazione di servizi IT gestiti, cybersecurity e soluzioni digitali al tessuto imprenditoriale B2B. La presente politica rappresenta l'espressione formale dell'impegno della Direzione Generale a perseguire un sistema di gestione della sicurezza delle informazioni efficace, appropriato al contesto organizzativo e coerente con gli indirizzi strategici aziendali.

L'organizzazione promuove la protezione degli asset informativi propri e dei clienti, contemperando le esigenze di sviluppo economico, creazione di valore e innovazione tecnologica con la salvaguardia della riservatezza, integrità e disponibilità delle informazioni. A tal fine, si impegna a rispettare la normativa vigente e i requisiti contrattuali applicabili, incoraggiando la diffusione di una cultura della sicurezza che coinvolga tutto il personale e le parti interessate.

Questa politica fornisce il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni e orienta l'intera architettura documentale del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), sostenendo il miglioramento continuo delle prestazioni e la capacità di adattamento ai cambiamenti del contesto interno ed esterno.

Campo di applicazione

La presente 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). Rientrano nel campo di applicazione tutte le funzioni organizzative — Area Tecnica, Helpdesk, Sistemistica MSP e Cloud, Development, Cybersecurity, Area Commerciale, Area Amministrazione e Customer Care — nonché i collaboratori esterni e i fornitori che accedono ai sistemi o alle informazioni aziendali nell'esecuzione dei propri servizi. Sono escluse le attività di lavoro da remoto, in quanto non previste dall'organizzazione.

Riferimenti normativi

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

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, integrità e disponibilità delle informazioni; può comprendere inoltre proprietà quali autenticità, responsabilità, non ripudio e affidabilità.
- **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.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Rischio per la sicurezza delle informazioni** : effetto dell'incertezza sugli obiettivi di sicurezza delle informazioni.
- **Controllo** : misura che modifica o riduce il rischio, incluse politiche, procedure, linee guida, pratiche o strutture organizzative.
- **Informazioni documentate** : informazioni che l'organizzazione è tenuta a controllare e mantenere, unitamente al supporto su cui sono contenute.
- **Non conformità** : mancato soddisfacimento di un requisito.
- **Azione correttiva** : azione volta a eliminare la causa di una non conformità e a prevenirne la ricorrenza.

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 le attività di comunicazione interna della politica e ne raccoglie le evidenze di diffusione.
- **Qualità GDPR NIS2 ISO 27001** : predispone le bozze di aggiornamento della politica, coordina la gestione dei rischi informativi e monitora l'efficacia dei controlli attuati.
- **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** : osserva le regole del SGSI, utilizza le risorse aziendali in modo appropriato e segnala tempestivamente eventi o debolezze di sicurezza.

Impegno e obiettivi del sistema di gestione

Impegno della Direzione

LANONE S.a.s, per il tramite della **Direzione Generale** , si impegna a stabilire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni, assicurando che esso rimanga appropriato alla missione aziendale di erogazione di servizi IT gestiti, cybersecurity e soluzioni digitali a clienti B2B. La Direzione assume la responsabilità ultima dell'efficacia del SGSI e ne promuove l'integrazione nei processi di business, affinché la sicurezza delle informazioni non costituisca un elemento isolato ma un fattore abilitante della strategia d'impresa.

L'organizzazione si impegna in particolare a:

- valutare e approvare le risorse — in termini di personale qualificato, infrastruttura tecnologica, strumenti di monitoraggio e programmi di formazione — necessarie a sostenere il SGSI in modo proporzionato ai rischi identificati;
- identificare e trattare sistematicamente i rischi e le opportunità che possono influire sulla riservatezza, integrità e disponibilità delle informazioni;
- soddisfare i requisiti legislativi, regolamentari e contrattuali applicabili, con particolare attenzione alla protezione dei dati personali;
- promuovere la consapevolezza e la competenza di tutto il personale attraverso programmi di formazione continua sulle minacce e sulle migliori pratiche di sicurezza;
- favorire la segnalazione di vulnerabilità e incidenti senza timore di ritorsioni, affinché ogni evento possa essere valutato, classificato e trattato tempestivamente;
- riesaminare periodicamente l'adeguatezza del SGSI nell'ambito del riesame di direzione, traducendo le lezioni apprese da incidenti e audit in azioni correttive concrete.

Principi fondanti

Il sistema di gestione si fonda su un approccio basato sul rischio: ogni decisione di sicurezza discende dalla valutazione strutturata delle minacce, delle vulnerabilità e degli impatti potenziali, con priorità assegnata in funzione della probabilità di occorrenza e della gravità delle conseguenze. La responsabilità condivisa permea l'intera organizzazione: la sicurezza delle informazioni è un dovere di ogni persona che opera all'interno dei sistemi aziendali o interagisce con essi. Il miglioramento continuo rappresenta il motore evolutivo del SGSI, alimentato dal monitoraggio degli indicatori di prestazione, dagli audit interni e dai riesami di direzione.

Obiettivi strategici di sicurezza delle informazioni

La presente politica fornisce il quadro entro cui sono determinati gli obiettivi di sicurezza delle informazioni, declinati come segue:

Obiettivo	Ambito
Garantire la protezione dei dati dei clienti B2B e delle infrastrutture gestite, preservando riservatezza, integrità e disponibilità in linea con gli obblighi contrattuali e i livelli di servizio concordati	Protezione dei clienti
Mantenere un approccio sistematico alla valutazione e al trattamento dei rischi, adottando tecnologie proporzionate al livello di rischio identificato — crittografia, backup ridondanti, vulnerability scanning, soluzioni EDR	Gestione del rischio

Assicurare la conformità ai requisiti legali, regolamentari e contrattuali applicabili, con particolare riguardo alla protezione dei dati personali	Conformità normativa
Promuovere la consapevolezza del personale mediante programmi di formazione continua su minacce e migliori pratiche di sicurezza	Competenza e consapevolezza
Garantire la continuità dei servizi IT critici attraverso piani di continuità operativa e di ripristino di emergenza periodicamente testati	Continuità operativa
Favorire il miglioramento continuo del SGSI tramite il monitoraggio degli indicatori di prestazione, gli audit interni e i riesami periodici della direzione	Miglioramento continuo

Comunicazione della politica

La presente politica è resa disponibile come informazione documentata e comunicata a tutto il personale interno attraverso email aziendale, piattaforma SharePoint, Microsoft Teams e incontri di team. Per le parti interessate esterne, la politica è accessibile tramite il sito web aziendale e le specifiche di fornitura contenute nei contratti con i clienti. L'uso di canali personali per la distribuzione della politica è espressamente vietato. Il **Responsabile del sistema di gestione** raccoglie le evidenze di avvenuta comunicazione — email inviate, ricevute di conferma, verbali di riunione — a garanzia della tracciabilità.

Archiviazione e aggiornamento

La presente politica è archiviata in formato digitale sulla piattaforma documentale aziendale e conservata sotto il controllo del **Responsabile del sistema di gestione** , che ne assicura la disponibilità, la protezione da modifiche non autorizzate e la rintracciabilità delle versioni precedenti. Il riesame della politica avviene con cadenza annuale oppure in occasione di cambiamenti significativi nel contesto organizzativo, normativo o tecnologico. La funzione **Qualità GDPR NIS2 ISO 27001** predispone la bozza di aggiornamento, che la **Direzione Generale** approva formalmente prima della pubblicazione e della successiva comunicazione a tutto il personale e alle parti interessate esterne.

Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Processi direzionali

- PRO Procedura gestione comunicazione
- PRO Procedura di gestione dei rischi
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Gestione riesame della direzione