

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Giampiero Pera	Fabrizio Sessarego

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Archiviazione e aggiornamento
- Documenti di riferimento

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi tecnologici e le sedi di Alet Communications Srl, con particolare riferimento alla sede operativa di Piazza Brignole 3/1, 16122 Genova. Essa coinvolge l'intero personale dell'organizzazione, inclusi dipendenti, collaboratori a contratto, fornitori e qualsiasi terza parte che abbia accesso alle informazioni o ai sistemi informativi aziendali, indipendentemente dalla modalità di lavoro — in sede, presso i clienti o da remoto.

In quanto provider di servizi ICT e di comunicazione per le imprese, Alet Communications gestisce quotidianamente informazioni critiche dei propri clienti business e della propria infrastruttura, che comprendono soluzioni di Unified Communications, networking, cybersecurity, connettività internet e servizi cloud. La protezione di tali asset informativi rappresenta un requisito essenziale per la continuità del business e per la fiducia delle parti interessate. Questa politica costituisce il documento quadro al vertice del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e stabilisce la cornice strategica entro cui operano tutte le altre politiche, procedure e controlli di sicurezza dell'organizzazione.

Riferimenti normativi

- **ISO/IEC 27001:2022:** Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO/IEC 27002:2022:** Linee guida per i controlli di sicurezza delle informazioni.
- **Regolamento (UE) 2016/679 (GDPR):** Protezione delle persone fisiche con riguardo al trattamento dei dati personali.
- **Direttiva (UE) 2022/2555 (NIS 2):** Misure per un livello comune elevato di cybersicurezza nell'Unione.
- **D.Lgs. 138/2024:** Recepimento della Direttiva NIS 2 nell'ordinamento italiano.

Termini e definizioni

- **Sicurezza delle Informazioni:** La tutela della riservatezza, integrità e disponibilità delle informazioni.
- **Riservatezza:** La proprietà per cui le informazioni non vengono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità:** La proprietà di salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- **Disponibilità:** La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **SGSI (Sistema di Gestione della Sicurezza delle Informazioni):** L'approccio sistematico dell'organizzazione per gestire le informazioni sensibili in modo che

rimangano sicure, comprensivo di persone, processi e tecnologie.

- **Asset informativo:** Qualsiasi risorsa che abbia valore per l'organizzazione in relazione alla gestione delle informazioni, inclusi dati, sistemi, infrastrutture, software e documentazione.
- **Rischio per la sicurezza delle informazioni:** La combinazione della probabilità che una minaccia sfrutti una vulnerabilità di un asset informativo e dell'impatto che tale evento produrrebbe sull'organizzazione.
- **Soggetto NIS:** Entità identificata come soggetto essenziale o importante ai sensi della Direttiva NIS 2, tenuta al rispetto degli obblighi di sicurezza informatica e di notifica degli incidenti ivi previsti.

Ruoli e responsabilità

- **Top management:** Definisce gli indirizzi strategici e gli obiettivi in materia di sicurezza delle informazioni e cybersicurezza, garantendo risorse adeguate, l'integrazione del SGSI nei processi aziendali e il riesame periodico per assicurarne efficacia, conformità e miglioramento continuo.
- **Responsabile del Sistema di Gestione:** Supervisiona la conformità complessiva della presente politica e del SGSI, coordinando l'attuazione dei controlli di sicurezza, la gestione della documentazione e il monitoraggio delle prestazioni attraverso audit interni e riesami periodici.
- **Punto di Contatto NIS 2:** Funge da interlocutore primario con l'Agenzia per la Cybersicurezza Nazionale (ACN), curando le comunicazioni obbligatorie, l'accesso alla piattaforma digitale e la trasmissione tempestiva delle notifiche di incidenti significativi.
- **Sostituto Punto di Contatto NIS 2:** Garantisce la continuità delle funzioni del Punto di Contatto NIS 2 in caso di indisponibilità del titolare, assicurando che gli obblighi di comunicazione verso l'ACN siano sempre assolti nei tempi previsti.
- **Sostituto Referente CSIRT:** Supporta il coordinamento delle risposte agli incidenti di cybersecurity e assume la piena responsabilità operativa della gestione degli incidenti qualora il referente primario non sia disponibile.
- **ICT-Progettazione:** Integra i requisiti di sicurezza delle informazioni nella progettazione e nell'implementazione delle soluzioni ICT destinate ai clienti e all'infrastruttura interna dell'organizzazione.
- **Responsabile Amministrativo:** Assicura che le operazioni amministrative e finanziarie siano condotte nel rispetto delle politiche di sicurezza delle informazioni e delle normative applicabili in materia di protezione dei dati.
- **Tutto il personale, collaboratori e terze parti:** Ogni persona che opera per conto di Alet Communications o che accede ai suoi sistemi informativi è tenuta a comprendere e applicare la presente politica, a rispettare i principi e le linee guida in essa contenuti e a segnalare immediatamente qualsiasi anomalia, evento sospetto o violazione della sicurezza delle informazioni attraverso i canali stabiliti dall'organizzazione.

Obiettivi di sicurezza delle informazioni

La dedizione di Alet Communications alla sicurezza delle informazioni rappresenta un pilastro strategico che si traduce in obiettivi chiari e misurabili, i quali guidano ogni decisione in materia. Il primo e fondamentale obiettivo è garantire una solida **conformità normativa**, nel pieno rispetto della ISO/IEC 27001, della Direttiva NIS 2 e del GDPR, nonché di tutti gli obblighi contrattuali assunti verso i clienti business, assicurando che le pratiche di sicurezza siano sempre allineate ai più recenti requisiti legali e regolamentari.

Al di là della conformità, lo scopo primario dell'organizzazione è la **protezione proattiva degli asset informativi**. Alet Communications opera quotidianamente gestendo infrastrutture di rete, soluzioni di comunicazione unificata, servizi cloud e piattaforme di cybersecurity per conto dei propri clienti; salvaguardare attivamente queste informazioni e la proprietà intellettuale aziendale da ogni minaccia, interna o esterna, costituisce un impegno imprescindibile. Questo impegno si estende all'obiettivo di garantire la **resilienza operativa**: l'organizzazione non si limita a prevenire gli incidenti, ma si prepara a rispondervi, mantenendo la continuità delle operazioni critiche e ripristinando i servizi in modo rapido ed efficace, così da minimizzare l'impatto sul business e sui clienti.

L'organizzazione riconosce che la tecnologia da sola non è sufficiente. Pertanto, un obiettivo cruciale è la **promozione di una cultura della sicurezza** pervasiva, in cui ogni membro del personale non sia soltanto a conoscenza delle politiche, ma comprenda profondamente il valore del proprio ruolo nella protezione delle informazioni. Tale obiettivo si persegue mediante programmi periodici di sensibilizzazione e formazione, incluse le certificazioni tecniche che il personale tecnico acquisisce regolarmente. Infine, tutte le iniziative di sicurezza sono guidate da un approccio maturo alla **gestione del rischio**, che permette di identificare, valutare e trattare le minacce in modo sistematico e prioritario, assicurando che le risorse siano investite dove possono generare il massimo valore per la protezione del patrimonio informativo aziendale.

Gli obiettivi di sicurezza delle informazioni sono riesaminati periodicamente nell'ambito del riesame della direzione e sono documentati nel *MOD Programma di miglioramento*, che ne specifica tempi, risorse, indicatori di monitoraggio e responsabilità. Il Top Management approva il piano di adeguamento che identifica gli interventi necessari e riceve relazioni periodiche sugli esiti di tali piani e sulla valutazione dell'efficacia delle misure di gestione del rischio.

Principi fondamentali di sicurezza delle informazioni

La strategia di sicurezza delle informazioni di Alet Communications non si fonda su un singolo controllo, ma su un insieme di principi interconnessi che costituiscono le fondamenta del SGSI.

Il pilastro su cui si regge l'intera struttura è il principio della **responsabilità condivisa**. La sicurezza delle informazioni non è un compito relegato ad un singolo reparto, ma un dovere che appartiene a ogni persona all'interno dell'organizzazione e a ogni terza parte che vi collabora. Per questo, Alet Communications promuove una cultura in cui ogni

dipendente, collaboratore e fornitore è consapevole del proprio ruolo ed è tenuto a segnalare tempestivamente qualsiasi incidente, debolezza o anomalia di sicurezza, nota o sospetta, attraverso i canali di comunicazione interni predisposti dall'organizzazione, quali e-mail, messaggistica interna e sistema di ticketing. L'organizzazione per la sicurezza informatica, con i relativi ruoli e responsabilità, è formalmente definita, approvata dagli organi di amministrazione e direttivi e resa nota a tutte le articolazioni competenti.

Questa responsabilità diffusa è guidata da un **approccio proattivo basato sulla gestione del rischio**. Le decisioni in materia di sicurezza delle informazioni non sono arbitrarie, ma derivano da un'analisi formale delle minacce e delle vulnerabilità, documentata nel *MOD Valutazione dei rischi di sicurezza delle informazioni*, che consente di implementare controlli proporzionati ed efficaci. L'organizzazione adotta una scala di valutazione del rischio basata su probabilità e impatto, con livelli definiti — basso, medio e alto — e una soglia di mitigazione oltre la quale è obbligatorio attuare misure di trattamento specifiche.

Uno dei principali frutti di questo approccio è il principio del **controllo degli accessi**: l'accesso alle informazioni e ai sistemi viene concesso seguendo le logiche di "minimo privilegio" e "necessità di sapere", assicurando che ogni utente disponga esclusivamente delle autorizzazioni indispensabili per svolgere le proprie mansioni. Le regole per l' **uso accettabile delle informazioni e delle risorse** associate sono formalmente documentate e comunicate a tutto il personale; ogni membro dell'organizzazione è tenuto a utilizzare gli asset informativi esclusivamente per finalità aziendali autorizzate, nel rispetto delle classificazioni di riservatezza stabilite. I beni aziendali utilizzati fuori sede — inclusi dispositivi portatili, supporti di memorizzazione e documentazione — devono essere protetti con misure adeguate al livello di classificazione delle informazioni in essi contenute, adottando precauzioni contro il furto, lo smarrimento e l'accesso non autorizzato.

I controlli, a loro volta, non sono elementi isolati. Il principio della **sicurezza integrata (security-by-design)** garantisce che la sicurezza sia una componente nativa e non un'aggiunta tardiva, venendo considerata fin dalla fase di progettazione di nuovi processi, sistemi o servizi ICT, tanto per l'infrastruttura interna quanto per le soluzioni erogate ai clienti. L'organizzazione adotta inoltre la regola della **scrivania pulita e dello schermo pulito**: le postazioni di lavoro devono essere libere da documenti e supporti contenenti informazioni sensibili quando non presidiate, e i dispositivi devono essere configurati con il blocco automatico dello schermo dopo un periodo di inattività, al fine di prevenire l'accesso non autorizzato o la divulgazione accidentale.

Infine, Alet Communications applica una strategia di **difesa in profondità**, implementando più livelli di controlli di sicurezza — tecnologici, fisici e procedurali. In questo modo, qualora una barriera dovesse risultare inefficace, altre sarebbero pronte a intervenire, creando una protezione stratificata e resiliente per gli asset più preziosi dell'organizzazione. La **cybersecurity è integrata nelle pratiche delle risorse umane**: il personale autorizzato ad accedere ai sistemi informativi rilevanti è individuato previa valutazione dell'esperienza, delle capacità e dell'affidabilità, e gli amministratori di sistema sono nominati con atto formale. Gli obblighi di sicurezza informatica sono definiti contrattualmente e permangono anche dopo la cessazione o la modifica del rapporto di lavoro.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI di Alet Communications. Essa è approvata dagli organi di amministrazione e direttivi dell'organizzazione e sarà riesaminata con cadenza almeno annuale, oppure a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia, nel contesto delle minacce o nel quadro normativo applicabile, sotto la supervisione del Responsabile del Sistema di Gestione.

Le modifiche alla politica sono gestite in conformità alla *PRO Procedura di gestione delle informazioni documentate* e sono tracciate mediante il *MOD Gestione del cambiamento*. Ogni nuova versione è comunicata a tutto il personale e alle terze parti interessate attraverso i canali di comunicazione interni ed esterni dell'organizzazione, affinché sia compresa, applicata e rispettata da tutti i soggetti coinvolti. I ruoli e le responsabilità in materia di sicurezza informatica sono riesaminati e, se opportuno, aggiornati almeno ogni due anni, nonché in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce.

Documenti di riferimento

- Codice di condotta
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica del sistema di gestione
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di conservazione e cancellazione delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione delle risorse umane
- PRO Procedura dei ruoli e responsabilità