Pubblico

POL Politica di sicurezza delle informazioni

15/06/2026

Indice

Scopo

La presente politica formalizza l'impegno del **CEO / Top Management** di Ambimed S.r.l. verso la protezione del patrimonio informativo aziendale e rappresenta il documento di riferimento per la sicurezza delle informazioni nell'ambito del Sistema di Gestione Integrato (SGI). Attraverso questo documento l'organizzazione dichiara la propria volontà di istituire, attuare, mantenere e migliorare in modo continuativo i controlli necessari a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni gestite per l'erogazione dei propri servizi.

Il documento definisce il quadro entro il quale si collocano le politiche specifiche e le procedure operative di sicurezza delle informazioni, assicurando coerenza con gli obiettivi strategici e con i requisiti normativi e contrattuali applicabili. I principi qui enunciati orientano le decisioni, le priorità e l'allocazione delle risorse dedicate alla protezione degli asset informativi, promuovendo una cultura nella quale la sicurezza rappresenta un valore condiviso a ogni livello dell'organizzazione.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici di Ambimed S.r.l., ivi comprese le piattaforme digitali proprietarie dedicate all'erogazione dei servizi. Il suo perimetro è la sede operativa di Via Cappuccini 16, 20122 Milano, e qualsiasi luogo dal quale il personale accede alle risorse aziendali in modalità di lavoro da remoto o durante trasferte.

Sono destinatari della politica tutti i dipendenti, i collaboratori a contratto, i consulenti e le terze parti che, a qualsiasi titolo, accedono alle informazioni o ai sistemi dell'organizzazione.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- 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.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Evento di sicurezza delle informazioni** : occorrenza identificata dello stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza o un malfunzionamento dei controlli.
- **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 e di minacciare la sicurezza delle informazioni.
- **Asset** : qualsiasi bene che abbia valore per l'organizzazione.
- **Vulnerabilità** : debolezza di un asset o di un controllo che può essere sfruttata da una o più minacce.
- **Minaccia** : causa potenziale di un incidente indesiderato che può provocare danni a un sistema o all'organizzazione.

Ruoli e responsabilità

- **CEO / Top Management** : approva la presente politica, ne assicura la coerenza con gli indirizzi strategici e garantisce la disponibilità delle risorse necessarie alla sua attuazione.
- **Responsabile del sistema di gestione** : coordina l'attuazione della politica, ne cura la revisione periodica e verifica l'allineamento con il contesto organizzativo e normativo.
- **Responsabile IT** : garantisce l'adeguatezza dei controlli tecnici e delle infrastrutture a supporto degli obiettivi di sicurezza dichiarati nella presente politica.
- **Operation Manager** : promuove l'applicazione dei principi di sicurezza nelle attività operative quotidiane e segnala eventuali criticità al **Responsabile del sistema di gestione** .
- **Responsabile HR** : assicura che il personale sia informato dei contenuti della politica e delle proprie responsabilità in materia di sicurezza delle informazioni.
- **Lavoratore** : rispetta i principi e gli obblighi stabiliti dalla presente politica e dalle disposizioni di sicurezza correlate.

Obiettivi di sicurezza delle informazioni

Ambimed persegue obiettivi di sicurezza coerenti con la propria missione di fornitore di soluzioni nel campo della prevenzione, della salute e della sicurezza sul lavoro, e con il profilo di rischio emerso dalla valutazione condotta nell'ambito del SGI. In particolare l'organizzazione:

- tutela la riservatezza dei dati sanitari, dei dati personali dei viaggiatori e delle informazioni riservate dei clienti, consentendo l'accesso esclusivamente alle figure autorizzate in ragione del proprio ruolo;

- preserva l'integrità delle informazioni gestite attraverso le piattaforme proprietarie e i sistemi interni, affinché i dati rimangano accurati, completi e protetti da alterazioni non autorizzate;
- garantisce la disponibilità dei servizi digitali e dei sistemi informativi, così da sostenere la continuità operativa e la qualità del servizio offerto ai clienti;
- mantiene la conformità ai requisiti legali, regolamentari e contrattuali applicabili, con particolare riguardo alla protezione dei dati personali;
- promuove la consapevolezza e la competenza di tutto il personale attraverso iniziative di formazione e sensibilizzazione periodiche, calibrate sull'evoluzione delle minacce;
- adotta un approccio basato sul rischio per orientare priorità, risorse e controlli, riesaminando periodicamente il livello di esposizione e l'efficacia delle misure in essere;
- favorisce il miglioramento continuo del SGI integrando le lezioni apprese dagli incidenti, dagli audit interni ed esterni e dal riesame della direzione.

Ciascun obiettivo è declinato in traguardi misurabili, dotati di indicatori di prestazione, responsabilità, risorse e tempi di attuazione, nell'ambito del processo descritto nella *Obiettivi e pianificazione per il loro raggiungimento* . I risultati vengono valutati almeno annualmente in occasione del riesame della direzione, che costituisce il momento di verifica e riallineamento delle priorità strategiche.

Principi fondamentali di sicurezza delle informazioni

Approccio basato sul rischio

Ambimed fonda ogni decisione in materia di sicurezza delle informazioni sull'analisi sistematica dei rischi, condotta secondo la metodologia definita nella *Procedura di gestione dei rischi* . L'organizzazione identifica le minacce e le vulnerabilità che possono compromettere i propri asset informativi, ne valuta probabilità e impatto e determina i trattamenti più appropriati, privilegiando la mitigazione attraverso controlli organizzativi, tecnici e fisici. Il rischio residuo è riesaminato periodicamente e portato all'attenzione del **CEO / Top Management** in sede di riesame della direzione, affinché le scelte strategiche riflettano costantemente il quadro di rischio aggiornato.

Classificazione e protezione delle informazioni

L'organizzazione riconosce che le informazioni possiedono livelli di sensibilità differenti e adotta un sistema di classificazione articolato nei livelli Riservato, Limitato e Pubblico, disciplinato dalla *Politica di classificazione ed etichettatura delle informazioni* . A ciascun livello corrispondono requisiti specifici di trattamento, trasmissione e conservazione; l'accesso è governato dal principio della necessità di conoscere e documentato nel *Registro degli utenti autorizzati all'uso delle informazioni* , in modo che le misure di protezione risultino sempre proporzionate al valore e alla criticità dei dati gestiti.

Uso accettabile delle informazioni e delle risorse

Ambimed promuove un utilizzo responsabile e consapevole delle informazioni e delle risorse associate. Le regole di uso accettabile, che disciplinano le modalità di impiego dei dispositivi aziendali, dei servizi cloud, dei supporti rimovibili e delle comunicazioni elettroniche, sono formalizzate nella *Politica di sicurezza operativa* . Ogni soggetto che accede alle risorse dell'organizzazione le utilizza esclusivamente per finalità coerenti con il proprio ruolo e nel rispetto delle disposizioni di sicurezza vigenti, contribuendo attivamente alla protezione del patrimonio informativo aziendale. L'assegnazione degli asset al personale avviene mediante il *Modulo di assegnazione dei beni* , che formalizza la presa in carico e la responsabilità di custodia da parte dell'assegnatario.

Scrivania pulita e schermo pulito

L'organizzazione adotta il principio della scrivania pulita e dello schermo pulito per ridurre il rischio di accesso non autorizzato, perdita o danneggiamento delle informazioni durante l'attività lavorativa quotidiana. Documenti classificati, supporti rimovibili e credenziali non possono rimanere esposti in assenza del personale assegnatario; le postazioni di lavoro prevedono il blocco automatico dello schermo dopo un periodo di inattività. Le regole operative di dettaglio sono specificate nella *Politica di sicurezza operativa* .

Segnalazione degli eventi di sicurezza delle informazioni

Ambimed riconosce nella tempestività della segnalazione un fattore determinante per contenere le conseguenze degli eventi di sicurezza. Ogni dipendente, collaboratore o terza parte comunica senza indugio qualsiasi evento osservato o sospetto che possa compromettere la riservatezza, l'integrità o la disponibilità delle informazioni aziendali, utilizzando i canali designati dall'organizzazione. Gli eventi segnalati sono registrati nel *Registro degli incidenti di sicurezza delle informazioni* e gestiti secondo le fasi di rilevamento, classificazione, contenimento, eradicazione e ripristino disciplinate dalla *Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Responsabilità condivisa

La sicurezza delle informazioni non è prerogativa di una singola funzione, ma un impegno trasversale all'intera organizzazione. Il **CEO / Top Management** ne assicura il presidio strategico, le funzioni operative ne curano l'attuazione quotidiana e ciascun membro del personale contribuisce con il proprio comportamento al mantenimento dei livelli di protezione attesi. L'assegnazione puntuale delle responsabilità di sicurezza ai diversi ruoli aziendali è formalizzata nella *Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* , garantendo che ogni persona conosca con chiarezza i propri obblighi e le modalità per assolverli.

Protezione degli asset fuori sede

Ambimed opera in un contesto nel quale gli asset informativi vengono talvolta utilizzati al di fuori della sede aziendale, durante trasferte, attività di smart working e collaborazioni con soggetti esterni. L'organizzazione si impegna a garantire un livello di protezione

equivalente a quello applicato in sede, indipendentemente dal luogo in cui le risorse sono impiegate.

I principi su cui si fonda la protezione degli asset fuori sede sono i seguenti:

- **Assegnazione e responsabilità** : ogni dispositivo consegnato al personale (notebook, smartphone, SIM, accessori) è tracciato attraverso il *Modulo di assegnazione dei beni* . L'assegnatario assume la piena responsabilità della custodia, della corretta manutenzione e della restituzione integra del bene.
- **Protezione tecnica** : i dispositivi destinati all'uso fuori sede sono dotati di cifratura completa del disco, autenticazione rafforzata, blocco automatico dello schermo dopo un periodo di inattività, software antivirus aggiornato e funzionalità di blocco o cancellazione da remoto. Viene richiesto che le reti Wireless a cui i dispositivi si collegano devono utilizzare almeno la cifratura WPA2 con credenziali personalizzate.
- **Custodia** : i dispositivi aziendali non possono essere lasciati incustoditi in veicoli, aree comuni di strutture ricettive, spazi di coworking o altri luoghi non protetti. In trasferta l'assegnatario ne assicura la custodia in ambienti chiusi e accessibili unicamente al personale autorizzato.
- **Segnalazione di smarrimento, furto o danneggiamento** : il personale segnala immediatamente al **Responsabile IT** qualsiasi smarrimento, furto o danneggiamento di un asset fuori sede. La segnalazione attiva le procedure di blocco remoto del dispositivo, di revoca degli accessi e di aggiornamento delle credenziali; l'evento è trattato come incidente di sicurezza delle informazioni e registrato nel *Registro degli incidenti di sicurezza delle informazioni* .
- **Restituzione** : al termine della trasferta, del progetto o del rapporto di lavoro, l'asset è restituito all'organizzazione nelle condizioni d'uso ricevute, secondo le modalità previste dal *Modulo di assegnazione dei beni* .

Le regole operative per il lavoro da remoto, la protezione fisica delle postazioni fuori sede, l'utilizzo dei canali di comunicazione sicuri e le eventuali disposizioni riguardanti i dispositivi personali sono dettagliate nella *Politica di sicurezza operativa* .

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGI, archiviato nel repository documentale aziendale e reso accessibile al personale attraverso i canali interni dell'organizzazione. Il **Responsabile del sistema di gestione** ne cura la revisione con cadenza almeno annuale, oppure in occasione di cambiamenti significativi nel contesto organizzativo, nel panorama normativo, nell'infrastruttura tecnologica o nello scenario delle minacce. Ogni aggiornamento è sottoposto all'approvazione del **CEO / Top Management** prima della pubblicazione e comunicato tempestivamente a tutto il personale e alle parti interessate pertinenti.

Documenti di riferimento

- Politica di classificazione ed etichettatura delle informazioni

- Politica di sicurezza operativa
- Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- Procedura di gestione degli incidenti di sicurezza delle informazioni
- Procedura di gestione dei rischi
- Obiettivi e pianificazione per il loro raggiungimento
- Modulo di assegnazione dei beni
- Registro degli incidenti di sicurezza delle informazioni
- Registro degli utenti autorizzati all'uso delle informazioni