POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	28/04/2026	Anton Morale	Matteo Trovò

Indice

Scopo

StepsConnect riconosce nella sicurezza delle informazioni un pilastro della propria strategia d'impresa. Nata nel 2019 con la missione di modernizzare i processi di selezione del personale ad alto volume attraverso l'intelligenza artificiale, l'organizzazione pone la protezione dei dati dei candidati, delle informazioni dei clienti e del codice sorgente della propria piattaforma cloud al centro di ogni scelta operativa e di sviluppo.

Con la presente politica l' **Alta Direzione** esprime i princìpi, gli impegni e gli indirizzi che orientano il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), affinché esso risulti appropriato al contesto organizzativo, al modello di business e alle aspettative delle parti interessate. L'organizzazione promuove un approccio in cui lo sviluppo economico, l'innovazione tecnologica e la creazione di valore si integrano con la tutela del patrimonio informativo, il pieno rispetto della normativa vigente e la diffusione di una cultura della sicurezza a ogni livello. La presente politica rappresenta il riferimento di alto livello che ispira l'intero corpo documentale del SGSI, a partire dalla *POL Politica di sicurezza delle informazioni* , che ne declina i princìpi in un quadro operativo dettagliato, e dalle procedure collegate.

Campo di applicazione

La presente politica si applica a tutte le attività di progettazione, sviluppo, erogazione e supporto di soluzioni software e tecnologie di intelligenza artificiale e automazione dei processi per la ricerca, selezione e gestione delle risorse umane svolte da StepsConnect. Il campo di applicazione comprende l'insieme degli asset informativi, i processi organizzativi, i sistemi tecnologici e l'infrastruttura cloud su cui opera la piattaforma. La politica si estende a tutto il personale (dipendenti, collaboratori e terze parti che accedono a informazioni o sistemi aziendali), indipendentemente dalla sede operativa, includendo la sede legale di Via Luigi Galvani 24, 15121 Alessandria e le postazioni di lavoro da remoto.

Riferimenti normativi

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

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : parte del sistema di gestione complessivo, fondata su un approccio basato sul rischio, finalizzata a stabilire, attuare, mantenere e migliorare la sicurezza delle informazioni.
- **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 di un'informazione.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Parte interessata** : persona od organizzazione che può influenzare, essere influenzata da, o percepirsi come influenzata da una decisione o attività.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni.
- **Politica** : intenzioni e orientamento di un'organizzazione espressi formalmente dalla sua alta direzione.
- **Informazione documentata** : informazione che un'organizzazione è tenuta a controllare e mantenere, unitamente al supporto sul quale è contenuta.

Ruoli e responsabilità

- **Alta Direzione** : approva la presente politica, ne verifica l'adeguatezza in sede di riesame della direzione e ne assicura la comunicazione a tutti i livelli dell'organizzazione e alle parti interessate pertinenti.
- **Responsabile del sistema di gestione** : cura la redazione, l'aggiornamento e la diffusione della presente politica, monitorandone l'applicazione e proponendo le revisioni necessarie sulla base del contesto organizzativo, dei risultati degli audit e delle valutazioni del rischio.

Impegno e obiettivi del sistema di gestione

Impegni dell'organizzazione

StepsConnect adotta un approccio alla sicurezza delle informazioni fondato sulla valutazione sistematica dei rischi, riconoscendo che la protezione del patrimonio informativo è una responsabilità che coinvolge ogni livello dell'organizzazione. L' **Alta Direzione** si impegna a rendere disponibili le risorse necessarie al raggiungimento degli obiettivi di sicurezza e a promuovere una cultura in cui la salvaguardia delle informazioni è parte integrante delle attività quotidiane di tutto il personale.

L'organizzazione persegue la preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni trattate, con particolare attenzione ai dati personali dei candidati e dei clienti, al codice sorgente della piattaforma e a ogni altro asset rilevante per la continuità del servizio. StepsConnect riconosce il valore della conformità ai requisiti normativi, regolamentari e contrattuali applicabili e promuove il rispetto delle disposizioni in materia di protezione dei dati personali e di sicurezza informatica, avvalendosi del supporto di un DPO designato e del monitoraggio costante dell'evoluzione del quadro legislativo.

La gestione dei rischi per la sicurezza delle informazioni si basa su un processo strutturato di identificazione, valutazione e trattamento, disciplinato dalla *PRO Procedura di gestione dei rischi* . Il processo prevede scale di probabilità e impatto definite, una soglia di tolleranza oltre la quale ogni rischio è sottoposto a trattamento e una rivalutazione periodica, oltre che in occasione di cambiamenti significativi nel contesto interno o esterno, come risulta dall' *Analisi del contesto* .

StepsConnect integra la sicurezza in ogni fase del ciclo di vita dello sviluppo software, dalla progettazione al rilascio in produzione, adottando princìpi di sviluppo sicuro e segregazione degli ambienti conformemente alla *PRO Procedura di sviluppo sicuro* . L'infrastruttura interamente cloud su cui opera la piattaforma richiede, inoltre, una gestione attenta dei rapporti con i fornitori di servizi ICT: l'organizzazione valuta le implicazioni di sicurezza e conformità dei servizi esternalizzati e ne monitora i livelli di servizio attraverso i processi definiti nella *PRO Procedura di gestione degli acquisti e delle terze parti* .

L'organizzazione favorisce la consapevolezza e la competenza del personale in materia di sicurezza delle informazioni attraverso programmi di formazione e sensibilizzazione adeguati ai ruoli e alle responsabilità assegnate, affinché ciascun collaboratore sia in grado di riconoscere e segnalare tempestivamente eventi anomali o potenziali vulnerabilità. StepsConnect tutela chi effettua segnalazioni in buona fede e considera il contributo attivo di ogni persona un elemento essenziale per l'efficacia dei controlli di sicurezza.

La garanzia della continuità operativa e della capacità di ripristino dei servizi critici in caso di eventi avversi costituisce un ulteriore impegno dell'organizzazione, perseguito attraverso la definizione di obiettivi di ripristino misurabili e la predisposizione di piani di continuità e disaster recovery, come descritto nella *PRO Procedura di continuità operativa e di ripristino di emergenza* .

L' **Alta Direzione** si impegna al miglioramento continuo del SGSI, avvalendosi dei risultati degli audit interni, delle valutazioni del rischio, degli indicatori di prestazione e delle evidenze emerse dal riesame della direzione per affinare costantemente i controlli e i processi di sicurezza.

Obiettivi di sicurezza delle informazioni

StepsConnect definisce obiettivi di sicurezza delle informazioni coerenti con la presente politica e con gli indirizzi strategici aziendali. Gli obiettivi sono formulati in modo misurabile, comunicati alle funzioni pertinenti e riesaminati periodicamente in sede di riesame della direzione, secondo quanto previsto dalla *PRO Gestione riesame della direzione* . Il quadro degli obiettivi si articola lungo le seguenti direttrici:

- preservare la riservatezza, l'integrità e la disponibilità delle informazioni gestite dalla piattaforma e dai processi aziendali, con specifica attenzione ai dati personali e al codice sorgente;
- assicurare la conformità ai requisiti legali, regolamentari e contrattuali applicabili, in particolare in materia di protezione dei dati personali;
- gestire i rischi per la sicurezza delle informazioni con un processo sistematico e documentato, trattando ogni rischio che raggiunga o superi la soglia di tolleranza stabilita dall'organizzazione;

- garantire la resilienza dei servizi critici, perseguendo obiettivi di ripristino definiti e verificati;
- sviluppare e mantenere la competenza del personale in materia di sicurezza delle informazioni, attraverso interventi formativi calibrati su ruoli e responsabilità;
- integrare la sicurezza nel ciclo di vita dello sviluppo software, dalla fase di progettazione al rilascio in produzione.

Il **Responsabile del sistema di gestione** monitora il raggiungimento degli obiettivi attraverso indicatori definiti e ne riferisce all' **Alta Direzione** in occasione del riesame della direzione, proponendo le azioni di miglioramento necessarie. L' **Alta Direzione** valuta i risultati conseguiti e, ove necessario, ridefinisce obiettivi e priorità per il ciclo successivo, garantendo così un processo ciclico di pianificazione, attuazione, verifica e miglioramento.

Archiviazione e aggiornamento

La presente politica è conservata come informazione documentata del SGSI e resa accessibile a tutto il personale attraverso i canali di comunicazione aziendali approvati, nel rispetto delle modalità stabilite dalla *PRO Procedura gestione comunicazione* . La distribuzione interna avviene tramite posta elettronica aziendale, piattaforme di condivisione documentale, messaggistica aziendale, riunioni di team e sessioni formative; ciascun destinatario sottoscrive una conferma di presa visione. La politica è altresì pubblicata sulle pagine pubbliche del sito web aziendale, collocata nel footer affinché sia scaricabile e consultabile da chiunque vi acceda, e resa disponibile a clienti e fornitori attraverso la documentazione contrattuale.

La revisione avviene almeno in occasione di ogni riesame della direzione, nonché a seguito di modifiche significative al contesto organizzativo, agli indirizzi strategici, ai risultati delle valutazioni del rischio o degli audit, come disciplinato dalla *PRO Processi direzionali* . Il **Responsabile del sistema di gestione** predispone la bozza di aggiornamento, che l' **Alta Direzione** esamina e approva formalmente. Ogni modifica è registrata nel registro delle revisioni, versionata e comunicata a tutto il personale e alle parti interessate pertinenti attraverso i canali approvati. Le versioni superate sono archiviate con indicazione della data di sostituzione e rese inaccessibili per l'uso operativo corrente.

Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di sviluppo sicuro
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Gestione riesame della direzione
- PRO Processi direzionali
- PRO Procedura gestione comunicazione

- Analisi del contesto