Politica di sicurezza delle informazioni

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Protezione degli asset fuori sede
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

Il presente documento formalizza l'impegno del Top Management di Pelliconi Italia SpA verso la protezione del patrimonio informativo aziendale e stabilisce il quadro strategico di riferimento per la sicurezza delle informazioni all'interno del Sistema di Gestione Integrato (SGI).

Pelliconi Italia SpA riconosce le informazioni come asset strategico a supporto della propria attività di progettazione e produzione di chiusure in metallo e plastica per i mercati globali del food, beverage, wine e spirits. Questa politica definisce gli obiettivi, i principi e gli indirizzi generali che guidano l'organizzazione nel preservare la riservatezza, l'integrità e la disponibilità delle informazioni, nell'assicurare la conformità ai requisiti normativi e contrattuali applicabili e nel perseguire il miglioramento continuo delle misure di protezione. Da questo documento discendono tutte le politiche specifiche, le procedure e le istruzioni operative in materia di sicurezza delle informazioni e cybersicurezza che compongono il quadro documentale del SGI.

Campo di applicazione

La presente politica si applica alla sede operativa di Pelliconi Italia SpA e copre l'insieme delle attività, dei processi produttivi e amministrativi, degli asset informativi, dei sistemi informativi e di rete dell'organizzazione. Coinvolge tutto il personale aziendale, inclusi dipendenti, collaboratori a contratto, consulenti e terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro adottata.

Riferimenti normativi

- ISO/IEC 27001
- Direttiva (UE) 2022/2555
- D.Lgs. 138/2024
- Regolamento (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 delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.

- **Asset informativo** : qualsiasi elemento che ha valore per l'organizzazione, inclusi informazioni, software, hardware e servizi coinvolti nel trattamento delle informazioni.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo volto a modificare il rischio attraverso la selezione e l'attuazione di misure appropriate.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa a 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 correlati che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **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.
- **Cybersicurezza** : insieme delle attività necessarie per proteggere la rete e i sistemi informativi, i loro utenti e le altre persone interessate dalle minacce informatiche.

Ruoli e responsabilità

- **CEO** : approva la presente politica e assume la responsabilità finale dell'accettazione del rischio residuo per la sicurezza delle informazioni; promuove presso il Consiglio di Amministrazione l'adozione della presente politica e l'allocazione di risorse adeguate alla protezione del patrimonio informativo.
- **Board Member** : verifica la coerenza della strategia di sicurezza delle informazioni con gli indirizzi aziendali e ne approva gli orientamenti nell'ambito del Consiglio di Amministrazione.
- **Corporate Digital & Information Director** : governa la componente di sicurezza delle informazioni del SGI, definendo le priorità tecniche e organizzative per l'attuazione della presente politica.
- **Responsabile Sistema di Gestione SGSI Punto di Contatto ACN Referente CSIRT** : coordina l'attuazione, il mantenimento e il miglioramento continuo del sistema di gestione della sicurezza delle informazioni e gestisce le comunicazioni con l'Agenzia per la Cybersicurezza Nazionale e il CSIRT Italia.
- **Sostituto Punto di Contatto ACN** : assicura la continuità delle interlocuzioni con l'Agenzia per la Cybersicurezza Nazionale in caso di assenza o indisponibilità del punto di contatto principale.
- **Responsabile del sistema di gestione** : supporta la gestione documentale del SGI e coordina il programma di audit interni a garanzia della conformità del sistema.

- **Corporate HR Director** : integra i requisiti di sicurezza delle informazioni e di cybersicurezza nelle pratiche di gestione delle risorse umane lungo l'intero ciclo di vita del rapporto di lavoro.
- **General Manager/Plant Manager** : assicura l'applicazione operativa della presente politica presso lo stabilimento, promuovendo la conformità ai requisiti di sicurezza in tutte le funzioni produttive e di supporto.

Obiettivi di sicurezza delle informazioni

Pelliconi Italia SpA persegue obiettivi strategici di sicurezza delle informazioni coerenti con la propria missione industriale, con il contesto di rischio e con gli obblighi normativi applicabili.

L'organizzazione si impegna anzitutto a proteggere la riservatezza, l'integrità e la disponibilità dell'intero patrimonio informativo, dai dati di produzione e di ricerca alle informazioni commerciali, finanziarie e relative al personale, affinché ogni informazione risulti accessibile esclusivamente ai soggetti autorizzati, sia mantenuta accurata e completa e resti fruibile quando necessario per il regolare svolgimento delle attività aziendali.

L'approccio alla gestione del rischio costituisce un elemento centrale della strategia di sicurezza. Pelliconi Italia SpA adotta una metodologia sistematica, fondata sul calcolo Probabilità per Impatto, per valutare e trattare i rischi di sicurezza informatica, mantenendo il rischio residuo entro le soglie di accettabilità definite dal **CEO** . Le valutazioni sono condotte con cadenza almeno annuale e aggiornate ogniqualvolta intervengano cambiamenti significativi nel contesto delle minacce, nell'organizzazione o nella tecnologia.

L'organizzazione persegue la piena conformità ai requisiti normativi applicabili e ne monitora costantemente l'evoluzione per adeguare tempestivamente le proprie misure di protezione. In quest'ottica, Pelliconi Italia SpA promuove una cultura diffusa di consapevolezza in materia di sicurezza delle informazioni, investendo nella formazione continua e nell'aggiornamento delle competenze di tutto il personale affinché ciascun collaboratore sia in grado di riconoscere le minacce informatiche e di contribuire attivamente alla protezione del patrimonio informativo aziendale.

L'impegno al miglioramento continuo si concretizza nell'identificazione sistematica di interventi di adeguamento a seguito dei riesami della direzione, degli audit interni e delle valutazioni del rischio. Tali interventi sono formalizzati nel *MOD Programma di miglioramento* e sottoposti all'approvazione degli organi di amministrazione e direttivi, che ricevono relazioni periodiche sullo stato di avanzamento e sugli esiti conseguiti.

Principi fondamentali di sicurezza delle informazioni

La presente politica si articola in un insieme di principi che orientano tutte le decisioni e le misure adottate dall'organizzazione per la protezione del patrimonio informativo. Tali principi informano l'intero quadro documentale del SGI, dalle politiche specifiche di settore alle procedure operative, e rappresentano il riferimento costante per valutare l'adeguatezza dei controlli di sicurezza implementati.

Organizzazione per la sicurezza informatica

Pelliconi Italia SpA definisce e mantiene un'organizzazione dedicata alla sicurezza informatica, approvata dagli organi di amministrazione e direttivi e resa nota alle articolazioni competenti dell'organizzazione secondo il principio della necessità di conoscere. I ruoli, le responsabilità e i correlati poteri sono formalizzati nel *MOD Organigramma* e nel *MOD Mansionario* , mentre la mappatura dettagliata delle responsabilità di sicurezza per ciascuna funzione aziendale è stabilita dalla *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* . L'organizzazione per la sicurezza informatica include il punto di contatto con l'Agenzia per la Cybersicurezza Nazionale e il relativo sostituto, nonché il referente CSIRT, come previsto dalla normativa di recepimento della Direttiva (UE) 2022/2555. I criteri e le modalità per l'identificazione e la formalizzazione dei ruoli sono disciplinati dalla *PRO Procedura dei ruoli e responsabilità* . L'assetto organizzativo è riesaminato e, ove opportuno, aggiornato almeno ogni due anni, nonché in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce.

Gestione del rischio

L'organizzazione fonda la propria strategia di sicurezza sull'identificazione, la valutazione e il trattamento sistematico dei rischi che possono compromettere la riservatezza, l'integrità o la disponibilità delle informazioni, adottando misure di mitigazione proporzionate al livello di rischio individuato. I criteri di accettabilità, le opzioni di trattamento e le modalità operative sono definiti dalla *POL Politica di gestione del rischio* e dalla *PRO Procedura di gestione dei rischi* ; le valutazioni sono documentate nel *MOD Valutazione dei rischi di sicurezza delle informazioni* .

Classificazione e uso responsabile delle informazioni

Pelliconi Italia SpA classifica il proprio patrimonio informativo in tre livelli di sensibilità (Riservato, Limitato e Pubblico), a ciascuno dei quali sono associati specifici requisiti di protezione per il trattamento, la trasmissione e la conservazione dei dati. Il framework di classificazione, le regole di etichettatura e i controlli di protezione per ciascun livello sono stabiliti dalla *POL Politica di classificazione ed etichettatura delle informazioni* . L'organizzazione promuove l'uso responsabile e appropriato delle informazioni e di tutte le risorse associate e definisce nella *POL Politica di sicurezza operativa* le regole per l'uso accettabile delle postazioni di lavoro, dei dispositivi e dei servizi informatici aziendali. La conservazione dei dati per le durate definite e la loro cancellazione sicura al termine del periodo di conservazione sono disciplinate dalla *POL Politica di conservazione e cancellazione delle informazioni* .

Gestione degli asset e dei servizi critici

L'organizzazione mantiene un censimento aggiornato dei propri asset informativi, che comprende hardware, software, servizi cloud e dispositivi OT/IoT, documentato nel *MOD Censimento risorse, infrastrutture, asset* , e ne gestisce l'intero ciclo di vita dalla configurazione allo smaltimento sicuro attraverso la *PRO Procedura di configurazione, gestione e smaltimento degli asset* . L'assegnazione formale degli asset al personale

avviene tramite il *MOD Modulo di assegnazione dei beni* , che definisce le responsabilità di custodia in capo all'assegnatario. Le attività e i servizi aziendali sono inoltre categorizzati per livello di impatto nel *MOD Categorizzazione delle attività e dei servizi NIS* , al fine di comprendere e comunicare i servizi critici dai quali dipendono le parti interessate e di mantenere un elenco aggiornato dei sistemi informativi e di rete rilevanti.

Scrivania pulita e schermo pulito

Per ridurre il rischio di divulgazione accidentale di informazioni sensibili, l'organizzazione adotta il principio della scrivania pulita e dello schermo pulito. Documenti e supporti di memorizzazione rimovibili contenenti informazioni classificate come Riservato o Limitato non sono lasciati incustoditi sulle postazioni di lavoro al termine dell'attività o in caso di assenza prolungata. I dispositivi aziendali sono protetti mediante blocco automatico dello schermo dopo quindici minuti di inattività. Le regole operative dettagliate sono definite nella *POL Politica di sicurezza operativa* .

Controllo degli accessi e gestione delle identità

Pelliconi Italia SpA adotta i principi del minimo privilegio e del controllo degli accessi basato sui ruoli per garantire che ciascun utente disponga esclusivamente delle autorizzazioni necessarie allo svolgimento delle proprie mansioni. L'intero ciclo di vita delle utenze, dalla richiesta alla creazione, dalla modifica alla revoca, è gestito attraverso la *PRO Procedura di gestione e controllo degli accessi logici* , che assicura la tracciabilità delle autorizzazioni e la revisione periodica dei diritti di accesso.

Affidabilità delle risorse umane

L'organizzazione integra la sicurezza delle informazioni in ogni fase del rapporto di lavoro. Il personale destinato ad accedere ai sistemi informativi e di rete rilevanti è individuato previa valutazione dell'esperienza, delle capacità e dell'affidabilità; gli amministratori di sistema sono selezionati con criteri di particolare rigore. I contratti di lavoro includono clausole relative agli obblighi di sicurezza informatica, riservatezza e protezione dei dati personali che permangono anche dopo la cessazione del rapporto. Al termine della collaborazione, l'organizzazione procede al recupero degli asset tramite il *MOD Modulo di restituzione dei beni* , alla revoca degli accessi e alla verifica degli adempimenti residui attraverso la *MOD Lista di controllo per uscita dei dipendenti* . Le pratiche di gestione delle risorse umane in relazione alla sicurezza sono disciplinate dalla *PRO Procedura di gestione delle risorse umane* , e il *Codice di condotta* vincola tutto il personale al rispetto delle politiche del SGI.

Segnalazione degli eventi e gestione degli incidenti

L'organizzazione predispone canali dedicati affinché tutto il personale possa segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni osservato o sospetto. Dipendenti, collaboratori e terze parti comunicano senza ritardo ogni anomalia o comportamento sospetto al **Responsabile Sistema di Gestione SGSI Punto di Contatto ACN Referente CSIRT** attraverso i canali definiti dall'organizzazione. Le segnalazioni

attivano il processo strutturato di gestione degli incidenti, dalla rilevazione al contenimento, dall'eradicazione al ripristino e all'analisi post-incidente, disciplinato dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* . Ogni evento è registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni* .

Sicurezza fisica e ambientale

Pelliconi Italia SpA protegge le proprie sedi, le aree sensibili e le apparecchiature da minacce fisiche e ambientali attraverso un approccio a più livelli che comprende perimetri di sicurezza, controlli degli accessi fisici per personale e visitatori e misure di protezione delle infrastrutture, secondo quanto definito dalla *PRO Procedura di sicurezza fisica e ambientale* .

Protezione delle reti, crittografia e monitoraggio

L'organizzazione garantisce la sicurezza dell'infrastruttura di rete attraverso la segmentazione, l'hardening dei dispositivi e il monitoraggio del traffico, in conformità alla *PRO Procedura di gestione della sicurezza della rete* . La crittografia è impiegata per proteggere la riservatezza e l'integrità delle informazioni durante il trattamento, la trasmissione e la conservazione, secondo i criteri stabiliti dalla *PRO Procedura di crittografia e gestione delle chiavi crittografiche* . Strumenti e processi dedicati alla registrazione e all'analisi degli eventi di sicurezza supportano l'individuazione tempestiva di attività anomale sui sistemi aziendali.

Gestione delle vulnerabilità e sviluppo sicuro

L'organizzazione identifica, valuta e corregge tempestivamente le vulnerabilità tecniche che possono interessare i propri sistemi informativi e di rete, al fine di ridurre la superficie di attacco e prevenire lo sfruttamento da parte di minacce informatiche. La sicurezza è integrata in ogni fase del ciclo di vita dello sviluppo software, dalla progettazione ai test e al rilascio in produzione, secondo i principi di security by design e by default definiti dalla *PRO Procedura di sviluppo sicuro* .

Continuità operativa e ripristino

Pelliconi Italia SpA si impegna a garantire la resilienza dei propri servizi critici adottando strategie di continuità operativa, piani di ripristino in caso di disastro e procedure di gestione delle crisi, formalizzati nella *POL Politica di continuità operativa* e nella *PRO Procedura di continuità operativa e di ripristino di emergenza* .

Sicurezza della catena di approvvigionamento

La sicurezza delle informazioni si estende alla catena di approvvigionamento dell'organizzazione. Pelliconi Italia SpA seleziona, qualifica e monitora i propri fornitori sulla base di criteri che includono la conformità ai requisiti di cybersicurezza e integra nei contratti clausole specifiche a tutela della riservatezza, dell'integrità e della disponibilità

delle informazioni. Le modalità operative sono disciplinate dalla *PRO Procedura di gestione degli acquisti e delle terze parti* .

Formazione e consapevolezza

L'organizzazione promuove un programma strutturato di formazione e sensibilizzazione in materia di sicurezza delle informazioni, rivolto a tutto il personale e differenziato per ruoli e responsabilità, al fine di sviluppare le competenze necessarie a prevenire e riconoscere le minacce informatiche. Le competenze acquisite sono verificate periodicamente e documentate nella *MOD Matrice delle competenze* .

Conformità normativa e audit

Pelliconi Italia SpA persegue la conformità costante ai requisiti normativi applicabili e ai requisiti del SGI attraverso il programma di audit interni disciplinato dalla *PRO Gestione audit interni* e le attività di misurazione e monitoraggio previste dalla *PRO Procedura delle misurazioni e del monitoraggio* . Il *MOD Elenco norme* è mantenuto aggiornato come riferimento per la verifica di conformità. I risultati delle valutazioni sono presentati nel riesame della direzione, documentato nel *MOD Verbale di riesame della direzione* , e contribuiscono all'identificazione delle azioni di miglioramento formalizzate nel *MOD Programma di miglioramento* .

Protezione degli asset fuori sede

Pelliconi Italia SpA riconosce che gli asset informativi utilizzati al di fuori delle proprie sedi (laptop, dispositivi mobili, supporti di memorizzazione rimovibili e documenti fisici affidati al personale in trasferta, in lavoro da remoto o consegnati a soggetti esterni) richiedono misure di protezione dedicate per compensare l'assenza dei controlli fisici e ambientali garantiti dalla sede aziendale.

L'organizzazione si impegna a garantire che ogni asset fuori sede sia soggetto a custodia responsabile da parte del personale assegnatario, che ne risponde per l'integrità e la sicurezza per tutta la durata dell'utilizzo. I dispositivi aziendali sono destinati esclusivamente a finalità lavorative e il personale assegnatario ne impedisce l'accesso a persone non autorizzate, indipendentemente dal luogo in cui vengono utilizzati.

Il trasporto degli asset avviene in custodia personale del soggetto assegnatario, adottando le precauzioni necessarie a prevenire smarrimento, furto o danneggiamento. In caso di necessità di consegna a sedi distaccate o a soggetti esterni, l'organizzazione prevede l'impiego di canali tracciabili.

Pelliconi Italia SpA richiede a tutto il personale di comunicare senza ritardo ogni evento di smarrimento, furto o danneggiamento di asset aziendali fuori sede al **Responsabile Sistema di Gestione SGSI Punto di Contatto ACN Referente CSIRT** , attivando le misure di contenimento previste, quali il blocco remoto del dispositivo e la revoca delle credenziali. Ogni evento di questo tipo è trattato come incidente di sicurezza delle informazioni, registrato e gestito in conformità alla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Al termine della trasferta, del progetto o del rapporto di lavoro, ogni asset è restituito all'organizzazione attraverso il *MOD Modulo di restituzione dei beni* . Le regole operative per la protezione degli asset fuori sede, il lavoro da remoto e l'uso sicuro dei dispositivi portatili sono dettagliate nella *POL Politica di sicurezza operativa* .

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGI, archiviato e gestito in conformità alla *PRO Procedura di gestione delle informazioni documentate* . La sua revisione avviene con cadenza almeno annuale, ovvero ogniqualvolta si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi, sotto la supervisione del **Responsabile Sistema di Gestione SGSI Punto di Contatto ACN Referente CSIRT** . Gli esiti di ciascun riesame sono conservati in un registro aggiornato.

La presente politica, unitamente a tutte le politiche di sicurezza delle informazioni del SGI, è approvata dagli organi di amministrazione e direttivi di Pelliconi Italia SpA e resa nota alle articolazioni competenti dell'organizzazione nel rispetto del principio della necessità di conoscere.

Documenti di riferimento

- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di gestione del rischio
- POL Politica di continuità 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 gestione delle risorse umane
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di crittografia e gestione delle chiavi crittografiche
- PRO Procedura di sviluppo sicuro
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione della sicurezza della rete

- PRO Procedura delle misurazioni e del monitoraggio
- PRO Gestione audit interni
- PRO Procedura dei ruoli e responsabilità
- PRO Procedura di gestione delle informazioni documentate
- Codice di condotta
- MOD Organigramma
- MOD Mansionario
- MOD Valutazione dei rischi di sicurezza delle informazioni
- MOD Censimento risorse, infrastrutture, asset
- MOD Categorizzazione delle attività e dei servizi NIS
- MOD Modulo di assegnazione dei beni
- MOD Modulo di restituzione dei beni
- MOD Registro degli incidenti di sicurezza delle informazioni
- MOD Lista di controllo per uscita dei dipendenti
- MOD Matrice delle competenze
- MOD Elenco norme
- MOD Programma di miglioramento
- MOD Verbale di riesame della direzione