Politica di Sicurezza delle Informazioni

Allegato 2 Manuale del SGI

L'Alta Direzione di Vecomp Spa riconosce l'importanza strategica della sicurezza delle informazioni per il successo e la sostenibilità del proprio business, per la tutela dei propri asset informativi e per la fiducia dei propri clienti, partner e dipendenti. In un contesto operativo sempre più digitalizzato e interconnesso, caratterizzato da minacce informatiche in continua evoluzione e da un quadro normativo stringente che include la Direttiva NIS 2 e il Regolamento Generale sulla Protezione dei Dati (GDPR), la protezione delle informazioni è considerata una priorità assoluta e una responsabilità fondamentale a tutti i livelli dell'organizzazione.

Pertanto, l'Alta Direzione si impegna formalmente a definire, implementare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme ai requisiti dello standard internazionale UNI CEI EN ISO/ IEC 27001:2024 e alle disposizioni legislative applicabili. Questo impegno si traduce nella definizione di obiettivi chiari, nell'allocazione delle risorse necessarie (finanziarie, tecniche e umane), nella promozione di una cultura della sicurezza diffusa e nella garanzia che le responsabilità relative alla sicurezza delle informazioni siano chiaramente definite e comunicate. L'Alta Direzione si assume la responsabilità ultima della sicurezza delle informazioni all'interno di Vecomp Spa e si impegna a riesaminare periodicamente la presente politica e l'efficacia complessiva del SGSI per assicurarne la continua idoneità, adeguatezza ed efficacia rispetto al contesto interno ed esterno, agli obiettivi strategici aziendali e ai requisiti delle parti interessate.

Principi Fondamentali (Riservatezza, Integrità, Disponibilità)

La politica di sicurezza delle informazioni di Vecomp Spa si fonda sui tre principi cardine universalmente riconosciuti:

- **Riservatezza:** Assicurare che le informazioni siano accessibili solo alle persone autorizzate. Vecomp Spa si impegna a proteggere le informazioni sensibili, proprietarie e i dati personali da accessi, divulgazioni o utilizzi non autorizzati, implementando controlli di accesso logici e fisici adeguati, meccanismi di cifratura e accordi di non divulgazione ove necessario.
- **Integrità:** Salvaguardare l'accuratezza, la completezza e l'affidabilità delle informazioni e dei metodi di elaborazione. Vecomp Spa adotta misure per prevenire modifiche, cancellazioni o corruzioni non autorizzate o accidentali dei dati, sia durante la trasmissione che durante l'archiviazione, attraverso controlli di validazione, meccanismi di controllo delle versioni e procedure di backup.
- **Disponibilità:** Garantire che le informazioni e le risorse associate siano accessibili e utilizzabili su richiesta da parte degli utenti autorizzati, quando necessario per lo svolgimento delle attività operative. Vecomp Spa implementa soluzioni per la continuità operativa e il disaster recovery, monitora le prestazioni dei sistemi e gestisce la capacità delle infrastrutture per assicurare la resilienza e la tempestiva disponibilità dei servizi informativi critici.

Questi tre principi guidano la definizione e l'implementazione di tutti i controlli di sicurezza all'interno dell'organizzazione.

Obiettivi Strategici di Sicurezza delle Informazioni

In linea con l'impegno dell'Alta Direzione e i principi fondamentali, Vecomp Spa definisce i seguenti

obiettivi strategici generali per la sicurezza delle informazioni, che forniscono il quadro di riferimento per la definizione di obiettivi specifici e misurabili a livello operativo:

- **Proteggere gli Asset Informativi:** Identificare, classificare e proteggere adeguatamente tutti gli asset informativi critici dell'organizzazione (dati, software, hardware, infrastrutture, documentazione, know-how) in
- base al loro valore, ai requisiti legali e contrattuali e ai rischi associati.
- **Garantire la Conformità Normativa:** Assicurare la piena conformità ai requisiti della norma UNI CEI EN ISO/ IEC 27001:2024, della Direttiva NIS 2, del GDPR e di tutte le altre leggi, regolamenti e obblighi contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali.
- **Prevenire e Gestire gli Incidenti:** Ridurre la probabilità e l'impatto degli incidenti di sicurezza attraverso
- l'implementazione di misure preventive, il monitoraggio continuo, la definizione di piani di risposta efficaci e la tempestiva notifica alle autorità competenti e alle parti interessate, ove richiesto (in particolare secondo NIS2 e GDPR).
- **Promuovere la Consapevolezza:** Sviluppare e mantenere un elevato livello di consapevolezza sulla sicurezza delle informazioni tra tutto il personale e i collaboratori, attraverso programmi di formazione e comunicazione continui, affinché comprendano le proprie responsabilità e contribuiscano attivamente alla protezione delle informazioni.
- **Assicurare la Continuità Operativa:** Garantire la capacità dell'organizzazione di continuare a operare e fornire servizi essenziali anche in caso di gravi incidenti o disastri, attraverso piani di continuità operativa e disaster recovery testati e aggiornati.
- **Gestire i Rischi della Catena di Approvvigionamento:** Valutare e gestire i rischi per la sicurezza delle informazioni derivanti dalle relazioni con fornitori e partner, assicurando che anch'essi adottino misure di sicurezza adeguate, in linea con i requisiti NIS2.
- **Migliorare Continuamente:** Monitorare le prestazioni del SGSI, valutare l'efficacia dei controlli, analizzare gli incidenti e le non conformità, e implementare azioni correttive e di miglioramento per aumentare costantemente il livello di sicurezza complessivo.

Questi obiettivi strategici saranno riesaminati periodicamente dall'Alta Direzione e declinati in obiettivi specifici, misurabili, raggiungibili, pertinenti e temporalmente definiti (SMART) per le diverse funzioni e processi aziendali.

Allineamento con il Contesto Organizzativo e gli Obiettivi di Business

La sicurezza delle informazioni non è un fine a sé stante, ma uno strumento fondamentale per supportare il raggiungimento degli obiettivi di business di Vecomp Spa. La presente politica e l'intero SGSI sono definiti tenendo conto del contesto specifico in cui opera l'organizzazione, incluse le esigenze e le aspettative delle parti interessate (clienti, dipendenti, fornitori, autorità di regolamentazione, soci), i fattori interni (cultura organizzativa, processi, tecnologie) ed esterni (mercato, concorrenza, quadro normativo, minacce).

L'implementazione di adeguate misure di sicurezza mira a:

- Abilitare processi di business sicuri ed efficienti. Proteggere la reputazione e l'immagine aziendale. Garantire la fiducia dei clienti e dei partner commerciali.
- Supportare l'innovazione e l'adozione di nuove tecnologie in modo sicuro. Ridurre le perdite finanziarie derivanti da incidenti di sicurezza.
- Assicurare la conformità legale e normativa, evitando sanzioni.

La strategia di sicurezza delle informazioni è quindi intrinsecamente legata alla strategia di business complessiva e contribuisce attivamente al suo successo.

Approvato dal Presidente
Il 07-02-2025