Politica per la Sicurezza delle Informazioni

Allegato 2 Manuale del SGI

Indice

Introduzione 2
1. Scopo e Campo di Applicazione 2
1.1. Scopo 2
1.2. Campo di Applicazione 2
1.3. Allineamento con il Contesto Organizzativo e gli Obiettivi di Business 2
2. Riferimenti Normativi e Contrattuali 3
3. Principi e Obiettivi Chiave di Sicurezza 4
3.1. Principi Fondamentali 4
3.2. Obiettivi Strategici 4
4. Struttura di Governance della Sicurezza 4
4.1. Ruoli e Responsabilità 4
5. Approccio alla Gestione del Rischio 6
6. Politiche specifiche di cybersecurity 6
7. Meccanismi di Conformità e Monitoraggio 6
8. Procedure di Revisione e Aggiornamento 7
9. Documentazione Correlata 7

NR. REVISIONE	REDAZIONE	DATA	DATA VERIFICA	APPROVAZIONE SIGLA
00	*Comitato di Sicurezza*	*07-02-2025*	*07-02-2025*	*Consiglio di Amministrazione*

NR. REVISIONE	MOTIVO DELLA REVISIONE	DATA EMISSIONE
01	*Adeguemento alla Direttiva NIS2*	04-12-2025

Politica per la Sicurezza delle Informazioni

Allegato 2 Manuale del SGI

Introduzione

La presente Politica stabilisce i principi, gli obiettivi e la struttura di governance che guidano Vecomp SPA nella protezione dei propri sistemi informativi e dei dati, assicurando la conformità normativa e la continuità operativa. Questo documento rappresenta l'impegno formale del Vertice Aziendale verso un approccio proattivo e responsabile alla sicurezza informatica, in linea con i valori di trasparenza, innovazione e sostenibilità di Vecomp.

1. Scopo e Campo di Applicazione

1.1. Scopo

Lo scopo di questa Politica è definire il quadro di riferimento per la gestione della sicurezza delle informazioni e dei Sistemi informativi all'interno di Vecomp. Gli obiettivi primari sono:

- **Proteggere gli asset informativi**, inclusi dati personali, proprietà intellettuale, dati finanziari e informazioni di progetto, da ogni minaccia interna o esterna, intenzionale o accidentale.
- **Garantire la riservatezza**, l'integrità e la disponibilità delle informazioni e dei servizi IT, supportando l'efficienza operativa e la continuità del business.
- **Assicurare la conformità** con le normative vigenti in materia di cybersecurity e protezione dei dati, nonché con gli obblighi contrattuali verso clienti e partner.
- **Promuovere una cultura della sicurezza** a tutti i livelli dell'organizzazione, aumentando la consapevolezza e la responsabilità individuale.

1.2. Campo di Applicazione

La presente Politica si applica a tutte le attività di Vecomp SPA. Il suo ambito include:

- **Tutto il personale:** dipendenti, amministratori, collaboratori a tempo determinato e indeterminato, consulenti e personale di terze parti che accede ai sistemi e alle informazioni di Vecomp.
- **Tutti gli asset informativi:** dati in formato digitale e cartaceo, software (applicativi, di sistema), hardware (server, PC, dispositivi mobili, apparati di rete) e infrastrutture IT.
- **Tutti i processi aziendali:** che creano, gestiscono, archiviano o trasmettono informazioni, con particolare attenzione ai processi legati alla gestione di commesse, e gestione del personale.

1.3. 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.

2. Riferimenti Normativi e Contrattuali

Vecomp SPA si impegna a operare nel pieno rispetto del quadro normativo e degli standard di riferimento. La presente Politica è allineata e integrata con le seguenti disposizioni:

Riferimento	Descrizione	Impatto sul Vecomp
Direttiva (UE) 2022/2555 (NIS 2)	Misure per un livello comune elevato di cybersicurezza nell'Unione.	In quanto operatore "IMPORTANTE"
Legge 138/2024	Disposizioni urgenti in materia di cybersicurezza nazionale.	Recepisce e rafforza il quadro NIS 2 in Italia, definendo responsabilità e meccanismi di coordinamento con le autorità nazionali (es. ACN).
Regolamento (UE) 2016/679 (GDPR)	Protezione delle persone fisiche con riguardo al trattamento dei dati personali.	Vecomp garantisce la protezione dei dati di dipendenti, clienti e fornitori, implementando misure tecniche e organizzative adeguate e gestendo i data breach.
D.Lgs. 101/2018	Disposizioni per l'adeguamento della normativa nazionale al GDPR.	Integra il GDPR nell'ordinamento italiano, specificando sanzioni e compiti dell'Autorità Garante.
D.Lgs. 231/2001	Responsabilità amministrativa degli enti.	La Politica si integra nel Modello Organizzativo 231 per prevenire reati informatici che potrebbero comportare una responsabilità diretta dell'ente.
Standard ISO	Norme internazionali per i sistemi di gestione.	La Politica si allinea alla struttura degli altri sistemi di gestione certificati (ISO 9001-ISO 27001).

3. Principi e Obiettivi Chiave di Sicurezza

3.1. Principi Fondamentali

La gestione della sicurezza in Vecomp si fonda sui seguenti principi:

- **Riservatezza:** Le informazioni devono essere accessibili solo al personale autorizzato. Particolare attenzione è rivolta ai dati delle aziende clienti, alla proprietà intellettuale e ai dati personali.
- **Integrità:** Le informazioni devono essere accurate, complete e protette da modifiche non autorizzate. L'integrità è cruciale per i dati di progetto, i dati contabili e i sistemi di controllo (ove presenti).
- **Disponibilità:** Le informazioni e i sistemi devono essere accessibili e utilizzabili quando richiesto. La disponibilità è vitale per garantire la continuità degli uffici.
- **Approccio basato sul rischio:** Le misure di sicurezza sono proporzionate al livello di rischio identificato per ciascun asset informativo.
- **Sicurezza** by Design e by Default: I requisiti di sicurezza sono integrati fin dalla fase di progettazione di nuovi sistemi, processi o servizi. Le configurazioni predefinite sono impostate per essere sicure.
- **Responsabilità (Accountability):** Ogni individuo è responsabile delle proprie azioni e dell'uso che fa degli asset informativi aziendali.
- **Miglioramento continuo:** La postura di sicurezza di Vecomp è soggetta a un processo di revisione e miglioramento costante per adattarsi a nuove minacce e contesti operativi.

3.2. Obiettivi Strategici

Per tradurre questi principi in azioni concrete, Vecomp si pone i seguenti obiettivi:

01. Implementare e mantenere un sistema di gestione del rischio informatico per identificare, valutare e trattare le minacce agli asset critici.
02. Garantire la continuità operativa per i processi di business critici, con particolare riferimento alla gestione dei progetti informatici presso i clienti, attraverso piani di disaster recovery e business continuity.
03. Assicurare la conformità normativa (NIS 2, GDPR) attraverso audit periodici, formazione e un'adeguata documentazione.
04. Ridurre il rischio di incidenti legati a errore umano attraverso un programma di formazione e sensibilizzazione continua per tutto il personale.
05. Proteggere le infrastrutture di rete e i dati scambiati con partner e clienti, garantendo la sicurezza della supply chain.

4. Struttura di Governance della Sicurezza

Per garantire l'efficace attuazione di questa Politica, viene definita la seguente struttura organizzativa con ruoli e responsabilità chiari.

4.1. Ruoli e Responsabilità

Ruolo	Responsabile/i	Principali Responsabilità
Consiglio di Amministrazione (CdA)	Vertice aziendale:	• Approva la Cybersecurity Policy e le sue revisioni. • Garantisce l'allocazione di risorse (finanziarie, umane, tecnologiche) adeguate.

Ruolo	Responsabile/i	Principali Responsabilità
		• Supervisiona l'efficacia complessiva del programma di sicurezza.
Comitato di Sicurezza	Organo strategico (Presidente, Responsabile IT, DPO, CISO, Resp. Sistemi Gestione)	• Definisce la strategia di cybersecurity • Supervisiona l'analisi del rischio e approvare i piani di trattamento. • Gestisce gli incidenti di Sicurezza maggiori. • Riferisce periodicamente al CdA sullo stato della sicurezza. • Riferisce periodicamente all'ODV
Responsabile dei Sistemi Informativi (RSI)	Funzione IT interna	• Implementa e gestisce le misure di sicurezza tecniche (firewall, antivirus, backup, etc.). • Monitora la rete e i sistemi per rilevare attività anomale. • Gestisce gli account utente e i privilegi di accesso. • Fornisce supporto tecnico per la risoluzione degli incidenti.
Responsabile Sicurezza Sistema Informativo (CISO)	Funzione di Responsabile della Sicurezza del Sistema Informativo	• Definisce strategie, politiche e controlli per proteggere dati, sistemi e infrastrutture da minacce interne ed esterne, • Garantisce conformità normativa e gestione efficace dei rischi cyber • Gestiscela risposta agli incidenti informatici
Data Protection Officer (DPO)	Funzione Responsabile Privacy designata	• Sorveglia l'osservanza del GDPR e della normativa privacy. • Fornisce pareri sulla valutazione d'impatto sulla protezione dei dati (DPIA). • Coopera con l'Autorità Garante e funge da punto di contatto.
Responsabili di Funzione	Responsabili di area	• Classifica le informazioni all'interno della propria area di competenza. • Garantisce che il proprio team rispetti le policy di sicurezza. • Segnala tempestivamente eventuali incidenti o vulnerabilità.
Tutto il Personale	Ciascun dipendente e collaboratore	• Legge, comprende e rispetta la presente Politica e le procedure associate. • Utilizza asset e strumenti aziendali in modo sicuro e responsabile. • Completa la formazione obbligatoria in materia di sicurezza. • Segnala immediatamente qualsiasi sospetto incidente di sicurezza.

Inoltre, il Sistema è gestito con i riferimenti NIS2:

Punto di Contatto	Funzione di contatto con ACN
Referente CSIRT	Funzione di contatto con CSIRT

5. Approccio alla Gestione del Rischio

Vecomp adotta un approccio strutturato alla gestione del rischio informatico, in linea con le best practice internazionali (ISO 27001) e i requisiti della direttiva NIS 2. Il processo si articola nelle seguenti fasi:

- **Identificazione degli Asset:** Mappatura e classificazione di tutti gli asset informativi (dati, software, hardware, processi) in base alla loro criticità per il business.
- **Identificazione delle Minacce e Vulnerabilità:** Analisi delle potenziali minacce (es. malware, phishing, guasti hardware) e delle vulnerabilità dei sistemi.
- **Valutazione del Rischio:** Stima della probabilità di accadimento di una minaccia e del
- potenziale impatto (economico, operativo, reputazionale, legale) su ciascun asset. Il rischio viene calcolato e prioritizzato.
- **Trattamento del Rischio:** Per ciascun rischio identificato, il Comitato di Sicurezza approva un piano di trattamento, che può consistere in:
- Mitigazione: Implementazione di controlli di sicurezza per ridurre la probabilità o l'impatto.
- Trasferimento: Trasferimento del rischio a terze parti (es. tramite assicurazioni o clausole contrattuali).
- **Accettazione:** Accettazione formale del rischio quando questo rientra nei livelli di tolleranza definiti dal management.
- **Eliminazione**: Eliminazione della fonte di rischio (es. dismettendo un sistema obsoleto).
- **Monitoraggio** e Revisione: Il processo di gestione del rischio è continuo. I rischi e l'efficacia dei controlli sono monitorati costantemente e rivalutati almeno una volta all'anno o a seguito di cambiamenti significativi.

6. Politiche specifiche di cybersecurity

L’adozione della presente Policy richiede la definizione e la documentazione di specifiche politiche, le quali rappresentano i requisiti minimi di implementazione previsti dalla presente Policy. Tali politiche vengono raccolte in un **Addendum Politica** (Allegato2.1), che costituisce parte integrante del presente documento.

7. Meccanismi di Conformità e Monitoraggio

Vecomp SPA assicura la conformità a questa Politica e alle normative applicabili attraverso i seguenti meccanismi:

- **Audit Interni ed Esterni:** Verranno condotti audit periodici per verificare l'adeguatezza e l'efficacia delle misure di sicurezza implementate. I risultati degli audit saranno presentati al Comitato di Sicurezza.
- **Indicatori di Performance (KPI):** Saranno definiti e monitorati specifici indicatori per misurare l'efficacia del programma di sicurezza (es. numero di incidenti, tempo di risoluzione, percentuale di personale formato).
- **Gestione degli Incidenti:** È in vigore una procedura formale per la gestione degli incidenti di sicurezza, che include le fasi di identificazione, contenimento, eradicazione, ripristino e analisi post-incidente. La procedura prevede la notifica obbligatoria alle autorità competenti (ACN per NIS 2, Garante Privacy per GDPR) nei tempi previsti dalla legge.
- **Non Conformità:** Le violazioni della presente Politica da parte del personale saranno gestite in conformità con il sistema disciplinare aziendale e le normative vigenti. Le non conformità tecniche o procedurali daranno origine ad azioni correttive tracciate e monitorate.

8. Procedure di Revisione e Aggiornamento

La presente Politica è un documento vivo, destinato a evolvere con l'azienda e il contesto delle minacce.

- **Revisione Periodica:** La Politica sarà revisionata e, se necessario, aggiornata con cadenza almeno annuale dal Comitato di Sicurezza.
- **Revisione Straordinaria:** Una revisione straordinaria sarà condotta in caso di:
    - Incidenti di sicurezza significativi.
    - Cambiamenti importanti nell'organizzazione, nei processi o nelle tecnologie di Vecomp.
    - Emanazione di nuove normative o aggiornamenti di quelle esistenti.
    - Risultati di audit che evidenzino carenze significative.

Ogni nuova versione della Politica sarà formalmente approvata dal Consiglio di Amministrazione, comunicata a tutto il personale e alle parti interessate pertinenti, e archiviata secondo le procedure di gestione documentale di Vecomp.

9. Documentazione Correlata

La presente Politica è il documento quadro da cui discendono Procedure operative, tra cui (elenco non esaustivo):

- Gestione del rischio
- Gestione degli Asset Aziendali
- Controllo Accessi
- Backup e Ripristino dei Dati
- Gestione degli Incidenti di Sicurezza Informatica
- Piano di Continuità Operativa e Disaster Recovery
- Politica sull'utilizzo dei dispositivi aziendali, posta elettronica
- Gestione Malware
- Gestione Documentazione
- Change Management