POLITICA
SICUREZZA DELLE INFORMAZIONI

REVISIONE	MOTIVO DELLA REVISIONE	DATA	REDATTO	APPROVATO
01	Prima emissione	05-01-2026	GM	CDA

SOMMARIO

Principio

La sicurezza delle informazioni è gestita in base al rischio, ai requisiti legali e normativi e alle esigenze aziendali.

Dichiarazione di impegno dell'amministratore delegato

L'Alta Direzione di e-cons srl 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 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.
sabilità ultima della sicurezza delle informazioni all'interno di e-cons srl 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.

Introduzione

La sicurezza delle informazioni protegge le informazioni che ci vengono affidate. Una gestione errata della sicurezza delle informazioni può avere un impatto negativo significativo sui nostri dipendenti, sui nostri clienti, sulla nostra reputazione e sulle nostre finanze. Grazie a un efficace sistema di gestione della sicurezza delle informazioni, possiamo

1. Garantire il rispetto dei nostri obblighi legali, normativi e contrattuali
2. Garantire che le persone giuste abbiano il giusto accesso ai dati giusti al momento giusto
3. Fornire protezione dei dati personali come definito dal GDPR
4. Essere buoni cittadini e custodi dei dati

Principi Fondamentali (Riservatezza, Integrità, Disponibilità)

La politica di sicurezza delle informazioni di e-cons srl si fonda sui tre principi cardine universalmente riconosciuti:

- Riservatezza: Assicurare che le informazioni siano accessibili solo alle persone autorizzate. e-cons srl 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. e-cons srl 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. e-cons srl 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, e-cons srl 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, 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 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 e-cons srl. 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.

Quadro normativo per la sicurezza delle informazioni

Il sistema di gestione della sicurezza delle informazioni si basa su un quadro di riferimento per la politica di sicurezza delle informazioni. In combinazione con questa politica, le seguenti politiche costituiscono il quadro di riferimento:

1. **Politica di sicurezza delle informazioni**(la presente politica)**
2. **Politica di controllo degli accessi**
3. **Politica di gestione delle risorse**
4. **Politica di gestione dei rischi**
5. **Politica di classificazione e trattamento delle informazioni**
6. **Politica di sensibilizzazione e formazione sulla sicurezza delle informazioni**
7. **Politica di utilizzo accettabile**
8. **Politica relativa alla pulizia della scrivania e dello schermo**
9. **Politica in materia di mobilità e telelavoro**
10. **Politica di continuità operativa**
11. **Politica di backup**
12. **Politica relativa a malware e antivirus**
13. **Politica di gestione delle modifiche**
14. **Politica sulla sicurezza dei fornitori terzi**
15. **Politica di miglioramento continuo**
16. **Politica di registrazione e monitoraggio**
17. **Politica di gestione della sicurezza della rete**
18. **Politica sul trasferimento delle informazioni**
19. **Politica di sviluppo sicuro**
20. **Politica di sicurezza fisica e ambientale**
21. **Politica di gestione delle chiavi crittografiche**
22. **Politica di controllo crittografico e crittografia**
23. **Politica relativa a documenti e registrazioni**
24. **Politica sugli incidenti significativi e raccolta di prove**
25. **Politica di gestione delle patch**
26. **Politica sui servizi cloud**
27. **Politica sui diritti di proprietà intellettuale**
28. **Politica AI**
29. **Politica di protezione dei dati**
30. **Politica di conservazione dei dati**

Ruoli e responsabilità in materia di sicurezza delle informazioni

La sicurezza delle informazioni è responsabilità di tutti: comprendere e rispettare le politiche, seguire le procedure e segnalare violazioni sospette o effettive. I ruoli e le responsabilità specifici per il funzionamento del sistema di gestione della sicurezza delle informazioni sono definiti e registrati nel documento **Ruoli assegnati e responsabilità in materia di sicurezza delle informazioni**

Monitoraggio

La conformità alle politiche e alle procedure del sistema di gestione della sicurezza delle informazioni è monitorata dal team di revisione della direzione, insieme a revisioni indipendenti condotte periodicamente dall'audit interno ed esterno.

Obblighi legali e normativi

L'organizzazione prende sul serio i propri obblighi legali e normativi e tali requisiti sono registrati nel documento **Registro dei requisiti legali e contrattuali**

Formazione e sensibilizzazione

Le politiche sono rese facilmente accessibili a tutti i dipendenti e agli utenti terzi. È in atto un piano di formazione e comunicazione per comunicare le politiche, i processi e i concetti relativi alla sicurezza delle informazioni. Le esigenze formative sono identificate e i requisiti formativi pertinenti sono riportati nel documento **Matrice delle competenze.**

Miglioramento continuo del sistema di gestione

Il sistema di gestione della sicurezza delle informazioni viene continuamente migliorato. La **politica di miglioramento continuo**definisce l'approccio dell'azienda al miglioramento continuo ed è in atto un processo di miglioramento continuo.**

Conformità alle politiche

Misurazione della conformità

Il team di gestione della sicurezza delle informazioni verificherà la conformità a questa politica attraverso vari metodi, inclusi, ma non limitati a, rapporti sugli strumenti aziendali, audit interni ed esterni e feedback al responsabile della politica.

Eccezioni

Qualsiasi eccezione alla politica deve essere approvata e registrata in anticipo dal responsabile della sicurezza delle informazioni e segnalata al team di revisione della direzione.

Non conformità

Un dipendente che abbia violato la presente politica potrà essere soggetto ad azioni disciplinari, fino al licenziamento.

Miglioramento continuo

La politica viene aggiornata e rivista nell'ambito del processo di miglioramento continuo.