

Politica del Sistema di Gestione
per la Sicurezza delle Informazioni

1. Scopo e campo di applicazione

Lo scopo del presente documento è quello di descrivere i principi generali di Sicurezza delle Informazioni definiti dall'organizzazione al fine di sviluppare un funzionale Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

1.1 Riferimento alle norme

Norme	Riferimento puntuale
ISO/IEC 27001:2022	Paragrafo 5 "LEADERSHIP" Sotto paragrafo 5.2 "L'alta direzione deve stabilire una politica per la sicurezza delle informazioni." Controllo A.5.1 - Politiche per la sicurezza delle informazioni

2. Scopo

Lo scopo del presente documento è quello di descrivere la Politica del sistema di gestione per la sicurezza delle informazioni (SGSI) dell'organizzazione

3. Politica

L'organizzazione ha deciso di conformare i propri processi per la sicurezza delle informazioni allo standard ISO/IEC 27001:2022 per quanto concerne la protezione delle informazioni inerenti:

Commercializzazione e assistenza di prodotti per la videosorveglianza

Le finalità del SGSI sono:

Con la presente politica l'organizzazione intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

1. Diffondere una cultura per la sicurezza delle informazioni

L'organizzazione ritiene che la più importante linea di difesa sia rappresentata dal personale dell'azienda, indipendentemente dal suo livello, e si basa sulla sensibilità, consapevolezza e

patrimonio conoscitivo dei singoli individui. La Direzione opera in tal senso un incoraggiamento continuo e sostiene l'esecuzione di processi periodici di adeguata formazione quali fattori fondamentali per ottenere una cultura della sicurezza diffusa tra il personale.

2. Prevenire gli incidenti

La prevenzione è una misura indispensabile per proteggere le informazioni aziendali, poiché mette al riparo l'organizzazione dalle conseguenze di un evento indesiderato che avrebbe potuto tradursi in danni economici, legali o di immagine. L'analisi preventiva e i test rivestono un ruolo fondamentale in questo contesto. È necessario quindi prevedere l'implementazione di una serie di misure preventive e di recovery dei dati volte a ridurre il rischio di danno causato da interruzioni del servizio.

3. Contenere le conseguenze degli incidenti e garantire la continuità operativa

In aggiunta alla prevenzione, la strategia complementare per ridurre al minimo i danni è la risposta immediata ad un incidente. Come per tutte le situazioni di emergenza, predisporre un piano con adeguate misure di reazione e gestione facenti riferimento ad azioni ben precise a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività, rende possibile intervenire con prontezza riportando rapidamente l'azienda nelle condizioni di normalità e limitando il prolungarsi nel tempo di situazioni dannose.

4. Migliorare in modo continuo la sicurezza delle informazioni

L'organizzazione si impegna a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione per la Sicurezza delle Informazioni, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere il patrimonio informativo aziendale.

5. Rispettare i requisiti contrattuali

Tutti i requisiti di sicurezza delle informazioni che hanno origine contrattuale o legale hanno una rilevanza strategica per le attività dell'organizzazione e di conseguenza il loro rispetto è centrale per il SGSI. Più in generale, tutti gli aspetti di sicurezza delle informazioni che possono influenzare l'immagine aziendale, sono indirizzati nell'ambito del SGSI.

6. Rispettare i requisiti cogenti e regolamentari

Infine, tutti i requisiti relativi alla sicurezza delle informazioni che hanno origine dal panorama regolatorio cogente o ne derivano, o sono previsti all'interno di norme adottate dall'organizzazione sono centrali per il SGSI. La Politica per la Sicurezza delle Informazioni deve essere soggetta a verifica periodica al fine di assicurare la conformità del SGSI con le norme o regolamenti adottati dall'organizzazione. La Politica per la Sicurezza delle Informazioni verrà modificata a seguito del cambio norma, ISO/IEC27001:2022

L'organizzazione si impegna ad un costante miglioramento del SGSI, tenendo conto che:

- L'esigenza nasce dalla necessità di rispondere alle molteplici richieste provenienti dall'esterno e dall'interno dell'organizzazione, inclusa la necessità di rispondere a quanto definito dal GDPR in materia di protezione dei dati personali di clienti e dipendenti.
- L'organizzazione ha individuato la figura del Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (di seguito RSGSI) e le interfacce per le tematiche di sicurezza delle informazioni verso le terze parti. Il RSGSI riporterà sugli andamenti e sullo stato della sicurezza delle informazioni con cadenza semestrale.
- L'organizzazione ha incaricato il reparto ICT aziendale con il supporto dei consulenti esterni degli aspetti tecnologici per la sicurezza delle informazioni ed il supporto alla definizione del SGSI. Il reparto IT svolge anche il ruolo di gestore delle anomalie tecniche e degli incidenti di sicurezza delle informazioni.
- L'organizzazione ha definito gli obiettivi per la sicurezza delle informazioni che vengono aggiornati in occasione del Riesame della Direzione o quando ritenuto necessario dalla Direzione. L'RSGSI è responsabile del loro monitoraggio e della rilevazione di eventuali anomalie rispetto a quanto predisposto.
- L'organizzazione predispone, con frequenza annuale, programmi di formazione e di audit interni per mezzo dei quali assicura il controllo del proprio SGSI.
- L'organizzazione si impegna al rispetto delle leggi e direttive in materia di protezione dei dati e di sicurezza delle informazioni nonché delle prescrizioni legislative applicabili ai propri servizi.
- IL RSGSI ed il personale sono focalizzati verso il miglioramento continuo del SGSI per mezzo della misurazione delle prestazioni, degli audit interni e del riesame.

4. Responsabilità per l'applicazione della politica

- L'RSGSI è responsabile di assicurare che il SGSI sia implementato e mantenuto in conformità con questa Politica e per garantire che tutte le risorse necessarie siano disponibili
- L'RSGSI è responsabile del coordinamento operativo del SGSI e della segnalazione delle prestazioni del SGSI
- La Direzione deve rivedere il SGSI almeno una volta all'anno o ogni volta che si verifica un cambiamento significativo e preparare verbali della riunione. Lo scopo del riesame della direzione è stabilire l'adeguatezza e l'efficacia del SGSI
- L'RSGSI, in collaborazione con il dipartimento HR dell'organizzazione, implementeranno programmi di formazione sulla sicurezza delle informazioni e di sensibilizzazione per i collaboratori
- La protezione dell'integrità, della disponibilità e della riservatezza nelle attività è responsabilità del proprietario/assegnatario di ciascun bene
- Tutti gli incidenti o i punti deboli di sicurezza devono essere segnalati ai RSGSI
- IL RSGSI definirà quali informazioni relative alla sicurezza delle informazioni saranno comunicate a quale parte interessata (sia interna che esterna), da chi e quando

- L'RSGSI è responsabile dell'adozione e dell'attuazione del piano di addestramento e sensibilizzazione, che si applica a tutte le persone che hanno un ruolo nella gestione della sicurezza delle informazioni.

La politica del SGSI è comunicata all'interno dell'organizzazione per mezzo di apposite sessioni formative e comunicazioni da parte del SSGSI. La politica può essere comunicata all'esterno (clienti, fornitori, autorità ecc.) ma solo dopo parere positivo da parte del RSGSI.

La presente Politica verrà rivista ed aggiornata dall'organizzazione ogniqualvolta vi si verifichino avvenimenti e cambiamenti sostanziali e verrà analizzata ad ogni Riesame della Direzione.