Politica di sicurezza

Politica di Sicurezza delle Informazioni (ISO 27001:2022)
1. Obiettivi e Principi Fondamentali della Sicurezza delle Informazioni
2. Ambito di Applicazione e Applicabilità
3. Governance della Sicurezza delle Informazioni
4. Gestione dei Rischi e Analisi delle Minacce
5. Controllo degli Accessi e Autorizzazioni
6. Protezione delle Infrastrutture IT e dei Dati
7. Gestione degli Incidenti di Sicurezza e Risposta
8. Formazione e Sensibilizzazione sulla Sicurezza
9. Monitoraggio e Audit della Sicurezza
10. Miglioramento Continuo della Politica di Sicurezza

Politica di Sicurezza delle Informazioni (ISO 27001:2022)

La **Politica di Sicurezza delle Informazioni** definisce le linee guida e le procedure che l'organizzazione adotta per proteggere i dati e le informazioni aziendali, in conformità con gli standard internazionali come la ISO 27001. L'obiettivo è garantire la riservatezza, l'integrità e la disponibilità delle informazioni e ridurre i rischi legati alla sicurezza delle informazioni.

Di seguito vengono descritti i principali aspetti di questa politica in 10 punti chiave.

---

1. Obiettivi e Principi Fondamentali della Sicurezza delle Informazioni

La **sicurezza delle informazioni** è un processo che coinvolge tutta l'organizzazione, dai dipendenti alla direzione, e ha come obiettivo la protezione dei dati aziendali da minacce interne ed esterne. Gli **obiettivi** principali della politica sono:

- **Protezione della riservatezza**: Garantire che le informazioni sensibili siano accessibili solo a chi è autorizzato.
- **Integrità dei dati**: Assicurarsi che i dati siano accurati e non alterati in modo non autorizzato.
- **Disponibilità delle informazioni**: Garantire che i dati siano accessibili e utilizzabili in caso di necessità.

Principi fondamentali:

- Adottare una **gestione del rischio** continua per proteggere tutte le risorse aziendali.
- **Conformità legale**: Rispettare le leggi e regolamenti applicabili, in particolare in materia di protezione dei dati personali (es. GDPR).

- **Responsabilità condivisa**: La sicurezza delle informazioni è una responsabilità che coinvolge tutti i livelli aziendali.

---

2. Ambito di Applicazione e Applicabilità

La politica si applica a tutte le informazioni trattate, archivate e trasferite all'interno dell'organizzazione, inclusi:

- **Dati digitali**: Archivi, database, sistemi informatici.
- **Dati cartacei**: Documenti e report.
- **Sistemi e infrastrutture IT**: Server, reti, dispositivi mobili e cloud.

Essa copre tutti i dipendenti, collaboratori, fornitori, e partner che gestiscono o accedono alle informazioni aziendali. Ogni entità esterna che trattasse dati sensibili deve essere vincolata a contratti specifici in materia di protezione dei dati.

---

3. Governance della Sicurezza delle Informazioni

La governance della sicurezza delle informazioni è definita dai seguenti ruoli e responsabilità:

- **Alta Direzione**: È responsabile della definizione, dell'approvazione e del supporto per la politica di sicurezza. La direzione garantisce la disponibilità delle risorse necessarie.
- **Chief Information Security Officer (CISO)**: È il principale responsabile della gestione della sicurezza delle informazioni, monitorando i rischi e coordinando le risposte agli incidenti di sicurezza.
- **Responsabili di Dipartimento**: Ogni responsabile di dipartimento è incaricato di implementare e monitorare la sicurezza all'interno delle proprie aree operative.
- **Tutti i dipendenti**: Ogni individuo che accede alle informazioni aziendali è responsabile della protezione dei dati e della segnalazione di qualsiasi vulnerabilità o incidente.

---

4. Gestione dei Rischi e Analisi delle Minacce

Il processo di gestione dei rischi si articola nelle seguenti fasi:

- **Identificazione dei rischi**: Rilevamento delle minacce potenziali, come attacchi informatici, perdite di dati, danni fisici alle infrastrutture.
- **Valutazione dei rischi**: Analisi della probabilità di accadimento e dell'impatto che ciascun rischio potrebbe avere sull'organizzazione.
- **Trattamento dei rischi**: Definizione di misure preventive, correttive o trasferimento del rischio, attraverso soluzioni assicurative o altre modalità.

Il trattamento dei rischi deve seguire il principio di **prevenzione** e **mitigazione** per ridurre la possibilità che si verifichino incidenti di sicurezza.

---

5. Controllo degli Accessi e Autorizzazioni

Il controllo degli accessi è fondamentale per garantire che le informazioni siano accessibili solo a chi è autorizzato. Le misure chiave includono:

- **Politiche di accesso basato sui ruoli**: Gli accessi sono concessi in base al ruolo del dipendente o collaboratore, limitando l'accesso ai dati strettamente necessari per le sue funzioni.
- **Autenticazione forte**: Implementazione di autenticazione a più fattori per l'accesso a sistemi critici e dati sensibili.
- **Gestione delle credenziali**: Le password devono essere sicure, uniche e cambiate periodicamente.

Inoltre, l'accesso deve essere **revocato immediatamente** quando un dipendente lascia l'azienda o cambia ruolo.

---

6. Protezione delle Infrastrutture IT e dei Dati

Le infrastrutture tecnologiche devono essere protette da minacce interne ed esterne mediante:

- **Crittografia dei dati**: Tutti i dati sensibili devono essere cifrati sia durante la trasmissione (ad esempio, tramite HTTPS o VPN) che durante l'archiviazione.
- **Firewall e sistemi di rilevamento intrusioni**: Questi sistemi sono fondamentali per monitorare e proteggere la rete aziendale da attacchi esterni.
- **Backup regolari**: I dati devono essere sottoposti a backup regolari, con copie memorizzate in luoghi fisici separati e sicuri per evitare la perdita di informazioni in caso di disastri.

Tutti i sistemi informatici devono essere aggiornati regolarmente per correggere vulnerabilità note e per migliorare la protezione contro nuovi rischi.

---

7. Gestione degli Incidenti di Sicurezza e Risposta

Un piano efficace di risposta agli incidenti deve essere pronto ad affrontare potenziali violazioni di sicurezza. Le fasi del piano includono:

- **Rilevamento e identificazione**: Monitoraggio attivo dei sistemi per individuare anomalie o segnali di attacchi.

- **Contenimento**: Una volta identificato un incidente, devono essere messe in atto misure per isolare l'incidente e limitare i danni.
- **Recupero**: Ripristino dei sistemi compromessi e delle operazioni aziendali, con particolare attenzione alla protezione dei dati durante il processo di recupero.
- **Comunicazione e reportistica**: Gli incidenti devono essere documentati e, se necessario, segnalati alle autorità competenti, come nel caso di violazioni dei dati sensibili.

---

8. Formazione e Sensibilizzazione sulla Sicurezza

La formazione è un elemento cruciale per mantenere alta la consapevolezza della sicurezza tra tutti i dipendenti. La formazione continua include:

- **Sessioni periodiche di sensibilizzazione**: Per informare e aggiornare il personale sulle minacce emergenti e sulle migliori pratiche di sicurezza.
- **Simulazioni di attacchi**: Testare la reattività dei dipendenti in situazioni di attacco (es. phishing).
- **Formazione obbligatoria sui rischi di sicurezza**: I dipendenti devono essere formati sulla gestione delle password, sulla protezione dei dispositivi mobili e sulla protezione della privacy.

---

9. Monitoraggio e Audit della Sicurezza

Per garantire l'efficacia delle misure di sicurezza, l'organizzazione deve effettuare:

- **Audit periodici**: Audit interni ed esterni per verificare che le politiche di sicurezza siano correttamente implementate e che non vi siano vulnerabilità nei sistemi.
- **Monitoraggio continuo**: Utilizzo di strumenti automatizzati per il monitoraggio in tempo reale dei sistemi e della rete aziendale, al fine di individuare tempestivamente attività sospette o incidenti di sicurezza.
- **Analisi delle performance**: Valutazione dei risultati ottenuti dalle misure di sicurezza per identificare opportunità di miglioramento continuo.

---

10. Miglioramento Continuo della Politica di Sicurezza

La sicurezza delle informazioni non è mai statica; richiede un **miglioramento continuo** per affrontare le nuove minacce emergenti. Il miglioramento continuo include:

- **Revisione periodica della politica**: La politica di sicurezza deve essere aggiornata periodicamente per riflettere i cambiamenti nell'ambiente tecnologico e normativo.

- **Valutazione delle nuove minacce**: Monitoraggio delle evoluzioni dei rischi e aggiornamento delle misure di protezione.
- **Integrazione di feedback**: I risultati degli audit, delle simulazioni di incidenti e delle segnalazioni dei dipendenti devono essere utilizzati per migliorare le pratiche di sicurezza.

Ogni modifica alla politica di sicurezza deve essere approvata dalla direzione e comunicata a tutti i membri dell'organizzazione.

Questa **Politica di Sicurezza delle Informazioni** fornisce le linee guida per garantire che tutte le risorse, i dati e i sistemi aziendali siano protetti da minacce e rischi, mantenendo la conformità alle normative legali e promuovendo un ambiente sicuro per tutti gli stakeholder.