SCOPO

Le informazioni devono essere sempre protette, qualsiasi sia la loro forma e comunque siano condivise, comunicate o memorizzate.

La Sicurezza delle Informazioni è la protezione di informazioni da una vasta gamma di minacce, al fine di garantire la business continuity, ridurre al minimo i rischi e massimizzare il guadagno di investimenti e opportunità.

CAMPO DI APPLICAZIONE

Questa politica sostiene l'organizzazione generale delle politiche per la sicurezza delle informazioni e si applica a tutta l'organizzazione.

OBIETTIVI

- **Rischi** strategici e operativi per la sicurezza delle informazioni sono **compresi e trattati** per raggiungere un livello accettabile per l'organizzazione;
- La **riservatezza** delle informazioni dei clienti, dello sviluppo del prodotto e dei piani di marketing è protetta;
- L'**integrità** dei documenti è conservata;
- Servizi web pubblici e reti interne soddisfano determinati livelli di **disponibilità**.

PRINCIPI

- Questa organizzazione effettua un'analisi dei rischi e può quindi tollerare situazioni che potrebbero non essere adeguatamente affrontate in organizzazioni gestite in modo diverso, a condizione che i rischi concernenti le informazioni siano capiti, monitorati e trattati, se necessario, come previsto dal Sistema di Gestione.
- Tutto il personale è reso consapevole e responsabile per quanto riguarda la sicurezza delle informazioni rilevanti connesse al proprio ruolo.
- Sono state assegnate risorse per il finanziamento dei controlli di sicurezza delle informazioni.
- Nella gestione complessiva di sistemi informativi viene analizzata la possibilità di un loro uso fraudolento.
- Sono disponibili evidenze oggettive sullo stato della sicurezza delle Informazioni.
- I rischi per la sicurezza delle informazioni sono monitorati e sono intraprese idonee azioni qualora eventuali cambiamenti generino rischi che non sono accettabili dall'organizzazione.
- Nel Sistema di Gestione sono descritti i criteri per la classificazione del rischio e il livello di accettabilità.
- Non saranno tollerate situazioni che pongono l'organizzazione in violazione di leggi e norme di legge.

RESPONSABILITÀ

- Il Responsabile della Sicurezza delle Informazioni:
  - fornisce supporto per l'organizzazione del personale;
  - garantisce che i verbali sullo stato della sicurezza delle informazioni siano disponibili;
  - agisce in caso di incidente delle informazioni;
- Ogni membro del personale ha responsabilità in materia di sicurezza delle informazioni come parte del proprio lavoro;
- L'Organizzazione, nella figura del Responsabile per la Sicurezza delle Informazioni, collabora con i propri fornitori (inclusi i fornitori di servizi cloud IaaS, PaaS e SaaS) al fine di monitorare e raccogliere informazioni sulle minacce e vulnerabilità più comuni (threat intelligence), al fine di prevenire o comunque mitigare il verificarsi di incidenti di sicurezza delle informazioni.

RISULTATI CHIAVE

- Gli incidenti di sicurezza delle informazioni non comporteranno costi gravi e imprevisti o un'interruzione di servizi e delle attività commerciali.
- Le perdite dovute a frodi saranno conosciute e confinate entro limiti accettabili.
- L'accettazione del cliente di prodotti o servizi non sarà influenzata negativamente da preoccupazioni legate alla sicurezza delle informazioni.

RELATIVE POLITICHE

Per la corretta implementazione del Sistema di Gestione sono state definite dall'organizzazione delle politiche specifiche, raccolte in allegato.

Allegati

Politica Utilizzo Accettabile
Politica Access Control
Politica Gestione Credenziali
Politica Clear Desk e Clear Screen
Politica Gestione Incidenti di Sicurezza
Politica per la Sicurezza delle Informazioni nella Supply Chain
Politica per la Protezione dei Dati Personali

BERGAMO, LÌ 10/10/2025 LA DIREZIONE / IL TITOLARE DI TRATTAMENTO