Politica Sicurezza Informazioni di Reti Spa

Reti S.p,A. è impegnata in un processo continuo di miglioramento dei servizi, al fine di distinguersi come fornitore di alto livello di professionalità ed evoluzione costante nella risposta alle richieste dei Clienti, nel pieno rispetto dei requisiti contrattuali e della normativa vigente.

Riconoscendo la sicurezza delle informazioni e la protezione dei dati personali come elementi fondamentali di tale processo, adotta un approccio proattivo per proteggere dati e informazioni propri e dei clienti, nonché le infrastrutture tecnologiche, fisiche, logiche e organizzative che li gestiscono.

Per Reti S.p.A., perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- **Riservatezza**: le informazioni devono essere salvaguardate da accessi non autorizzati e utilizzate esclusivamente da soggetti debitamente autorizzati. La protezione deve essere assicurata sia nella fase di trasmissione che di conservazione.

- **Integrità**: le informazioni devono essere accurate, complete e non alterate. Sono implementati controlli rigorosi per garantire che i dati siano trattati in modo affidabile e protetti da modifiche non autorizzate, mantenendo la loro integrità nel tempo.

- **Disponibilità**: le informazioni devono essere reperibili in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica;

Reti S.p.A. promuove una Politica di Sicurezza delle Informazioni che ha alla base i seguenti obiettivi fondamentali e distintivi:

- **Garanzia di riservatezza, integrità e disponibilità delle informazioni**: assicura la protezione delle informazioni gestite nell'ambito di interesse, adottando misure di sicurezza adeguate a prevenire accessi non autorizzati, alterazioni e interruzioni di servizio.
- **Gestione dei rischi**: implementa un metodo sistematico di valutazione e trattamento dei rischi, identificando e mitigando le minacce alla sicurezza delle informazioni.
- **Implementazione di controlli di sicurezza**: seleziona, progetta e implementa controlli di mitigazione dei rischi di sicurezza efficaci, adattati alle specifiche esigenze aziendali.
- **Verifica dell'efficacia dei controlli**: conduce verifiche periodiche per garantire l'efficacia dei controlli di sicurezza implementati, identificando eventuali lacune e adottando misure correttive.
- **Miglioramento continuo del sistema di gestione della sicurezza**: riesamina l'adeguatezza dei controlli e l'efficacia del sistema di gestione della sicurezza delle informazioni, apportando miglioramenti continui in risposta all'evoluzione delle minacce, del business, del contesto tecnologico e normativo.
- **Sensibilizzazione del personale**: garantisce che tutto il personale sia informato delle proprie responsabilità nella gestione delle informazioni, promuovendo una cultura della sicurezza e della privacy.
- **Aumento della fiducia dei clienti**: rafforza la fiducia dei Clienti, dimostrando l'impegno nella protezione delle loro informazioni e dei loro dati personali.
- **Conformità agli standard ISO 27001 e ISO 27701**: adotta gli standard ISO 27001 per l'implementazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e ISO 27701 per il Sistema di Gestione delle Informazioni sulla Privacy (PIMS), perseguendo la conformità e la certificazione.

La Direzione si impegna a raggiungere tali obiettivi, assicurando la disponibilità delle risorse necessarie per l'implementazione e il mantenimento del SGSI e del PIMS, promuovendo una cultura della sicurezza e della privacy attraverso la sensibilizzazione e il coinvolgimento attivo del personale.

La Direzione, con il supporto delle funzioni aziendali, definisce le strategie per la sicurezza delle informazioni e l'attuazione della Politica di Sicurezza delle Informazioni, assicurando un monitoraggio costante e un miglioramento continuo.

Busto Arsizio, li 6 Marzo 2025