POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Scopo

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Sacchetto s.p.a. al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni, in linea con lo standard internazionale ISO/IEC 27001:2022.

Descrizione

Per Sacchetto s.p.a. la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS, attraverso il rispetto delle seguenti proprietà:

1. Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. Integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. Autenticità: garantire una provenienza affidabile dell'informazione.
6. Privacy: garantire la protezione ed il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con l'Organizzazione nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati. In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e terzi;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità dei dati/informazioni gestiti dall'organizzazione e la salvaguardia della proprietà intellettuale.

Ambito di applicazione

La politica per la sicurezza delle informazioni di Sacchetto s.p.a. si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa e commercializzazione nell'ambito dei servizi aziendali.

Principi della politica

La politica della sicurezza rappresenta l'impegno dell'organizzazione nei confronti tutte le parti interessate a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni dell'Organizzazione garantisce:

1. che l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. che l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
6. che l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
10. che i trattamenti dei dati personali avvengano nel rispetto del Regolamento UE 2016/679;
11. l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione SGSI (sistema di gestione della sicurezza delle informazioni);
12. il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa;
13. la selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.
14. il miglioramento continuo del Sistema di gestione per la sicurezza delle informazioni.

La politica per la sicurezza delle informazioni è formalizzata nel SGSI, viene costantemente verificata e riesaminata in sede di Riesame annuale della direzione ed all'occorrenza aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le parti interessate, attraverso un sistema intranet e specifici canali di comunicazione.

Responsabilità

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

La Direzione ha inoltre individuato un Responsabile del sistema di gestione per la sicurezza delle informazioni chiamato ad assicurare che il Sistema di gestione adottato sia definito, attuato, implementato e mantenuto in accordo con la norma ISO/IEC 27001:2022

Lagnasco, lì 13/01/2025

La Direzione
Giuliano SACCHETTO