Politica del Sistema di Gestione della Sicurezza delle Informazioni

ISO 27001

Piazza della Croce Rossa, 1 00161 Roma

FSTechnology S.p.A. – Gruppo Ferrovie dello Stato Italiane
Società per Azioni
Sede legale: Piazza della Croce Rossa, 1 – 00161 Roma
Capitale Sociale Euro 27.578.244,00
Iscritta al Registro delle Imprese di Roma
Cod. Fisc. e numero iscrizione 15032391003 – R.E.A. 1564073

1. Scopo e Contesto

FSTechnology, come **centro di competenza digitale** del Gruppo Ferrovie dello Stato Italiane, ha la missione di accelerare la **trasformazione digitale** e garantire la **resilienza operativa** delle infrastrutture tecnologiche. In questo contesto, la tutela del patrimonio informativo del Gruppo e dei nostri clienti è un fondamento imprescindibile della nostra strategia e un fattore chiave per la fiducia delle nostre parti interessate.

Questa politica stabilisce la visione, i principi guida e l'impegno dell'Alta Direzione per la sicurezza delle informazioni. Il nostro Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conforme alla norma internazionale **ISO/IEC 27001:2022**, è il framework attraverso cui governiamo i rischi e proteggiamo le informazioni in modo sistematico e proattivo nell'ambito dei servizi certificati verso il cliente Trenitalia.

2. I Nostri Principi Fondamentali di Sicurezza

Il nostro approccio alla sicurezza si basa sulla protezione dei tre pilastri fondamentali di ogni informazione che trattiamo:

- **Riservatezza:** Assicuriamo che le informazioni siano accessibili solo a chi è legittimamente autorizzato.
- **Integrità:** Salvaguardiamo l'accuratezza e la completezza delle informazioni e dei processi con cui vengono gestite.
- **Disponibilità:** Garantiamo che gli utenti autorizzati possano accedere alle informazioni e ai servizi correlati quando necessario.

3. I Nostri Impegni Strategici

Per attuare i nostri principi, l'Alta Direzione si impegna a:

- **Adottare un Approccio Basato sul Rischio:** Gestire la sicurezza attraverso un processo continuo di valutazione dei rischi, per assicurare che le misure di controllo siano sempre adeguate alle minacce e commisurate al valore delle informazioni da proteggere.
- **Garantire la Conformità:** Assicurare il pieno rispetto degli obblighi contrattuali, delle leggi e dei regolamenti vigenti in materia di sicurezza e protezione dei dati.
- **Promuovere la Cultura della Sicurezza:** Sviluppare e mantenere un'elevata consapevolezza della sicurezza a tutti i livelli dell'organizzazione, attraverso formazione e comunicazione continua, affinché ogni persona sia consapevole del proprio ruolo e delle proprie responsabilità.

- **Integrare la Sicurezza nel Ciclo di Vita dei Servizi:** Progettare e sviluppare i nostri sistemi e servizi secondo i principi di "Security by Design" e "Security by Default", integrando i requisiti di sicurezza in ogni fase, dall'acquisizione allo sviluppo e alla manutenzione.
- **Assicurare la Continuità Operativa:** Predisporre e mantenere piani di continuità operativa per garantire la resilienza dei servizi critici a fronte di incidenti o eventi avversi.
- **Perseguire il Miglioramento Continuo:** Riesaminare periodicamente l'efficacia del nostro SGSI e delle nostre performance di sicurezza per identificare e attuare sistematicamente opportunità di miglioramento.

3.1 Aree di Applicazione della Sicurezza

Per dare attuazione pratica a questi impegni, l'organizzazione ritiene di fondamentale importanza l'adozione di adeguate misure di sicurezza, con particolare riferimento alle seguenti aree:

- **Conformità** alle disposizioni di Gruppo e legislative vigenti in materia.
- **Individuazione di ruoli e responsabilità** nella gestione della sicurezza delle informazioni.
- **Formazione** e **consapevolezza** del personale sulle tematiche di sicurezza.
- **Classificazione e gestione del patrimonio informativo** in base alla sua criticità per il business.
- **Utilizzo corretto e sicuro** degli strumenti informatici aziendali.
- **Controllo degli accessi logici** alle informazioni, alle reti ed ai sistemi ICT.
- **Gestione sicura dell'operatività e delle comunicazioni** nell'elaborazione e trasmissione delle informazioni.
- **Gestione sicura dell'acquisizione, sviluppo e manutenzione** del patrimonio informativo.
- **Protezione fisica** dei siti in cui risiede il patrimonio informativo.
- **Gestione degli incidenti di sicurezza** delle informazioni.
- **Mantenimento della continuità operativa** dei servizi a seguito di eventi avversi.

La tutela della sicurezza del patrimonio informativo aziendale è assicurata tramite l'attività combinata delle funzioni aziendali. Per garantire la sicurezza delle informazioni, FSTechnology si raccorda con le specifiche unità organizzative del Gruppo FS Italiane, integrando il contributo di clienti e terze parti.

4. Quadro di Riferimento per gli Obiettivi di Sicurezza

Questa politica fornisce il quadro di riferimento per la definizione e il riesame degli obiettivi misurabili per la sicurezza delle informazioni. I requisiti e i principi generali di sicurezza sono contestualizzati all'interno

dell'organizzazione tramite obiettivi di carattere operativo finalizzati a supportare la realizzazione e il mantenimento del SGSI ISO27001.

L'organizzazione definisce obiettivi specifici, in linea con i principi qui espressi, che vengono formalizzati, monitorati tramite indicatori (KPI) e riesaminati almeno annualmente in sede di Riesame della Direzione per valutarne il raggiungimento e la continua pertinenza.

5. Comunicazione e Applicabilità

Questa politica si applica a tutte le informazioni, i processi e le risorse tecnologiche inclusi nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni. Viene comunicata a tutto il personale e resa disponibile alle parti interessate rilevanti.

L'Alta Direzione si assume la piena responsabilità di guidare, sostenere e verificare l'applicazione di questa politica, assicurando che la sicurezza delle informazioni sia una responsabilità condivisa a tutti i livelli dell'organizzazione.

L'AD
Erminio Marco Iacomussi