POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La sicurezza e la salvaguardia del patrimonio informativo costituiscono condizione imprescindibile per il successo del business, la continuità operativa e la fiducia degli stakeholders di Fandis S.p.A..
I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi aziendali e il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) rappresenta lo strumento che consente la condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni a livelli accettabili.

In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo un adeguato grado di:

- Riservatezza: proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati;
- Integrità: proprietà relativa alla salvaguardia dell'accuratezza e della completezza delle informazioni e dei beni ad esse collegati;
- Disponibilità: proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata;

delle informazioni attraverso l'adozione di un formale "Sistema di Gestione per la Sicurezza delle Informazioni" (SGSI) in linea con i requisiti attesi dagli stakeholders di Fandis S.p.A. e nel rispetto delle normative vigenti.

In particolare, il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di Fandis S.p.A. copre le attività di "Progettazione, produzione, commercializzazione di componenti e dispositivi per il controllo della temperatura di apparecchiature elettromeccaniche ed elettroniche e di sistemi di zanzariere e schermi solari."

Gli obiettivi generali del SGSI perseguiti con l'impegno della direzione, sono:

- minimizzare il rischio di perdita e/o indisponibilità dei dati gestiti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua e adeguata analisi dei rischi che identifichi, valuti e tratti periodicamente i rischi Cyber e di sicurezza informatica, esaminando costantemente le vulnerabilità e le minacce associate alle attività del sistema al fine di ridurre l'esposizione sia a fattori interni che esterni;
- promuovere programmi di formazione e sensibilizzazione (Cyber Security Awareness) per tutto il personale, accrescendone la consapevolezza e riducendo il rischio legato al fattore umano (es. Phishing);
- promuovere la collaborazione, comprensione e consapevolezza del SGSI da parte dei fornitori strategici;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere;
- conformarsi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera l'azienda, tra i quali, in particolare le regolamentazioni inerenti ai trattamenti dei dati personali e la loro sicurezza (GDPR e normative nazionali);

- garantire una risposta tempestiva agli incidenti di sicurezza attraverso l'applicazione di procedure operative collaudate di rilevamento, segnalazione e gestione degli stessi, al fine di minimizzare l'impatto sul business e ripristinare rapidamente la normale operatività.

Tutto il personale, nell'ambito delle relative responsabilità, è coinvolto nella segnalazione di eventuali eventi negativi o incidenti riscontrati e di qualsiasi debolezza identificata nel SGSI.

Tutta l'organizzazione, a partire dai vertici, è impegnata a supportare l'implementazione, la messa in opera e il riesame periodico per il miglioramento continuo del SGSI.

Il vertice aziendale si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica.

Borgo Ticino,
19 Maggio 2026

La Direzione
Silvano Zilioli