DATA F. SRL, punto di riferimento per le lavorazioni di precisione, si impegna costantemente a operare in conformità ai principi ESG e ad adottare politiche per lo sviluppo sostenibile.

Il nostro impegno per la protezione dei dati e la continuità operativa

La sicurezza delle informazioni rappresenta un elemento fondamentale per la tutela del patrimonio aziendale, dei dati dei clienti, dei partner e di tutte le parti interessate.

La nostra organizzazione adotta un approccio strutturato alla gestione della sicurezza delle informazioni, ispirato ai principi della norma internazionale ISO/IEC 27001, con l'obiettivo di garantire elevati standard di protezione, affidabilità e continuità operativa.

Il nostro approccio alla sicurezza

Proteggere le informazioni significa garantire:

- Riservatezza, assicurando che i dati siano accessibili solo alle persone autorizzate;
- Integrità, mantenendo le informazioni corrette, complete e protette da modifiche non autorizzate;
- Disponibilità, garantendo che sistemi e dati siano accessibili quando necessario;
- Affidabilità, attraverso processi controllati e monitorati;
- Continuità operativa, anche in presenza di eventi imprevisti o incidenti informatici.

La sicurezza delle informazioni viene integrata nei processi aziendali, nelle attività operative e nelle decisioni strategiche.

Sistema di Gestione per la Sicurezza delle Informazioni

La nostra organizzazione applica specifiche procedure per garantire la sicurezza delle informazioni finalizzate a:

- identificare e gestire i rischi legati alle informazioni;
- proteggere dati, infrastrutture e servizi digitali;
- prevenire accessi non autorizzati e violazioni;
- monitorare costantemente le minacce cyber;
- garantire il miglioramento continuo delle misure di sicurezza.

L'approccio adottato si basa sulla valutazione periodica dei rischi e sull'implementazione di controlli organizzativi, fisici e tecnologici adeguati.

Protezione dei dati e degli accessi

Per garantire un elevato livello di sicurezza adottiamo misure specifiche dedicate alla protezione delle informazioni e dei sistemi aziendali, tra cui:

- gestione controllata degli accessi;
- autenticazione sicura degli utenti;
- protezione delle reti e delle infrastrutture IT;
- monitoraggio dei sistemi informatici;
- backup periodici e procedure di ripristino;
- aggiornamento e gestione delle vulnerabilità;
- strumenti di protezione contro malware e minacce informatiche.

L'accesso alle informazioni avviene secondo il principio del minimo privilegio, assicurando che ogni utente possa accedere esclusivamente alle risorse necessarie per il proprio ruolo.

Formazione e consapevolezza

La sicurezza delle informazioni è anche una responsabilità condivisa.

Per questo motivo promuoviamo attività di formazione e sensibilizzazione rivolte al personale, con l'obiettivo di sviluppare consapevolezza sui rischi informatici e sulle corrette pratiche di sicurezza.

La diffusione di una cultura orientata alla sicurezza contribuisce a prevenire incidenti e a rafforzare la protezione dell'intera organizzazione.

Gestione degli incidenti e continuità operativa

La nostra organizzazione dispone di procedure dedicate alla gestione degli incidenti di sicurezza, finalizzate a:

- identificare rapidamente eventuali anomalie;
- limitare gli impatti operativi;
- ripristinare i servizi in tempi adeguati;
- analizzare le cause e prevenire il ripetersi degli eventi.

Sono inoltre adottate misure di business continuity e disaster recovery per garantire la continuità dei servizi e la resilienza operativa.

Conformità normativa

L'organizzazione opera nel rispetto delle normative applicabili in materia di protezione dei dati e sicurezza delle informazioni, inclusi gli obblighi previsti dal Regolamento UE 2016/679 (GDPR) e dagli altri requisiti normativi e contrattuali applicabili.

Miglioramento continuo

La sicurezza delle informazioni è un processo in continua evoluzione.

Per questo motivo monitoriamo costantemente l'efficacia delle misure adottate attraverso:

- audit interni;
- verifiche periodiche;
- monitoraggio dei rischi;
- analisi degli incidenti;
- aggiornamento continuo dei controlli di sicurezza.

L'obiettivo è migliorare nel tempo la capacità dell'organizzazione di prevenire, rilevare e gestire le minacce informatiche.