



POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

L'Organizzazione si impegna a garantire il raggiungimento degli obiettivi aziendali attraverso la piena adesione, da parte di tutti i collaboratori, ai principi identificati nel Sistema di Gestione per la Sicurezza delle Informazioni, ai requisiti della norma ISO/IEC 27001:2022 e a quelli legislativi, normativi e regolamentari applicabili.

La presente Politica per la Sicurezza delle Informazioni è ispirata ai seguenti principi fondamentali:

- ❖ Garantire la protezione delle informazioni attraverso il rispetto costante dei principi di Riservatezza, Integrità e Disponibilità (RID), applicati a tutte le attività aziendali, ai processi interni, ai sistemi IT, ai servizi erogati e ai dati dei clienti;
- ❖ Soddisfare i requisiti delle parti interessate, in particolare del cliente, attraverso l'offerta di prodotti e servizi che rispondano efficacemente alle loro esigenze in termini di affidabilità, continuità operativa e sicurezza delle informazioni;
- ❖ Promuovere il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni, attraverso il monitoraggio sistematico delle prestazioni, l'analisi dei rischi, gli audit interni, il riesame della Direzione e l'adozione di azioni correttive e preventive efficaci;
- ❖ Valutare e mitigare i rischi per la sicurezza delle informazioni, tramite un processo strutturato di identificazione, analisi e trattamento dei rischi, garantendo l'adozione di misure tecniche e organizzative idonee e proporzionate;
- ❖ Assicurare la conformità alle norme vigenti, agli obblighi contrattuali, ai requisiti legali e regolatori applicabili, inclusi quelli relativi alla protezione dei dati e alla cybersecurity;
- ❖ Rendere disponibili risorse e competenze adeguate per assicurare l'attuazione efficace delle misure di sicurezza, promuovendo la consapevolezza, la formazione e la responsabilizzazione di tutto il personale;
- ❖ Garantire la continuità operativa dei servizi critici, pianificando, testando e aggiornando i piani di business continuity e gestione degli incidenti in modo da minimizzare l'impatto di eventuali interruzioni o minacce;
- ❖ Monitorare e gestire gli incidenti di sicurezza, adottando procedure strutturate per l'identificazione, la segnalazione, l'analisi e la risoluzione degli eventi, al fine di ridurre i rischi residui e prevenire il ripetersi;
- ❖ Promuovere l'innovazione e l'aggiornamento tecnologico, mantenendo le infrastrutture e le soluzioni informatiche allineate agli standard di settore e alle best practices in materia di sicurezza delle informazioni.

La Direzione di **Softech**, con il pieno coinvolgimento di tutti i collaboratori, si impegna a **comunicare, diffondere e attuare** i principi di questa Politica, rendendola **disponibile a tutte le parti interessate** e garantendone il riesame periodico per verificarne la continua adeguatezza ed efficacia.

Gallarate, 24 novembre 2025

La Direzione di Softech S.r.l.

Mauro Roncari