POLITICA PER LA SICUREZZA DELLE INFORMAZIONI
ISO/IEC 27001:2022 – TISAX:ISA6

La politica della sicurezza delle informazioni dei sistemi ISMS (Information Security Management System) e TISAX (Trusted Information Security Assessment eXchange) è incentrata sulla volontà dell'Organizzazione di proteggere le informazioni alle minacce (interne, esterne, deliberate, accidentali, ambientali) e dalle vulnerabilità che possono comprometterle, garantendo primariamente che siano preservate le caratteristiche di Riservatezza, l'integrità e la Disponibilità delle informazioni stesse.
Tale volontà è resa operativa grazie alle risorse che la Direzione mette a disposizione per l'implementazione dei sistemi che consentono di perseguire tale obiettivo.

In particolare, per tutti i sistemi e i processi dell'organizzazione a supporto dei sistemi ISMS e TISAX, la Direzione assicura che:

- le informazioni siano accessibili esclusivamente alle persone autorizzate, siano esse interne che esterne all'azienda, garantendo livelli di servizio e complessità di accesso adeguati ai requisiti di sicurezza definiti per le informazioni;
- qualunque sia il formato delle informazioni trattate, sia garantita la loro disponibilità, integrità e riservatezza nel rispetto dei requisiti dei sistemi di gestione adottati e nel rispetto dei requisiti legali applicabili;
- sia effettuato un monitoraggio costante nel cambiamento degli asset e della tecnologia al fine di identificare tempestivamente nuove vulnerabilità;
- sia effettuato un costante aggiornamento sui siti specializzati in tematiche di sicurezza delle informazioni e forum per la pronta individuazione di nuove tipologie di minacce;
- sia prestata particolare attenzione alle variazioni dei requisiti normativi, legislativi, contrattuali ed alle relative priorità in relazione a nuovi sviluppi applicativi, se previsti;
- sia garantita la continuità operativa dell'IT, attraverso interventi mirati di tipo tecnico-organizzativo e che tali interventi siano definiti, costantemente aggiornati e periodicamente verificati;
- tutto il personale sia formato sulla sicurezza delle informazioni, che sia informato della necessità del rispetto delle politiche e dei regolamenti aziendali in tema di inforsec e che sia altresì sensibilizzato sulle conseguenze derivanti dalla violazione di tali politiche e regolamenti;
- siano effettuate valutazioni periodiche dell'efficacia dei sistemi di gestione per la sicurezza delle informazioni e della formazione dei collaboratori attraverso periodici assessment nell'ambito di applicazioni ed infrastruttura ICT (Vulnerability Assessment, Penetration Test, simulazioni di intrusione sulla sicurezza fisica, test di conoscenza delle policy, simulazioni di violazioni delle stesse, ecc);
- vengano introdotte metriche per la valutazione delle prestazioni dei sistemai di gestione ISMS e TISAX (KPI);
- vengano gestiti processi critici per la sicurezza delle informazioni (separazione dei ruoli, seprazione degli ambienti di sviluppo, test e produzione, segregazione delle reti, ecc)
- siano ridotti il più possibile i rischi alla fonte;
- qualsiasi violazione della sicurezza, reale o presunta, sia comunicata ed investigata;
- siano prontamente identificati e gestiti gli incidenti sulla sicurezza delle informazioni ed attivate le autorità competenti per quelli che hanno impatto su requisiti di legge violati;
- sia evitato l'utilizzo di software non autorizzati;
- siano effettuati riesami periodici (audit) dei sistemi di gestione per la sicurezza delle informazioni in modo indipendente finalizzati a:
  - verificare l'attualità e l'efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi;
  - verificare l'efficacia dei controlli attuati rispetto alla riduzione del livello di rischio;
  - controllare le modifiche apportate dalla tecnologica (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico, introduzione di nuovi rischi);
  - controllare le modifiche apportate alla configurazione dei sistemi ICT;
  - rivalutare periodicamente il livello di rischio dell'organizzazione, con particolare attenzione all'infrastruttura e ai sistemi ICT

L'organizzazione ha definito una metodologia di valutazione del rischio basata sulle linee guida della ISO/IEC 27005:2022 ed ha definito gli obiettivi finalizzati al mantenimento di un elevato standard di sicurezza delle informazioni.

La responsabilità dell'istituzione e della gestione dei sistemi di gestione della sicurezza delle informazioni (ISMS e TISAX) è assegnata al Responsabile per la Sicurezza delle Informazioni.

Pont-Saint-Martin, 30 maggio 2025

Responsabile per la Sicurezza Informazioni	*Direzione Generale*
Igor Zanetti	*A.Furfaro*