

TESISQUARE® ha come obiettivo la creazione di soluzioni di collaboration tra i business partner tramite soluzioni applicative che permettano ai partner stessi di raggiungere i propri obiettivi di business in maniera efficace ed efficiente.

TESISQUARE® in conformità alla normativa vigente, si è dotata di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) per il seguente campo di applicazione:

Design and provision of solutions for: supplier relationship management, collaborative transportation management, customer collaboration, dematerialization and optimization of business processes, electronic invoicing, EDI services, compliant document storage.

Le finalità del SGSI sono:

- **assicurare la riservatezza, l'integrità e la disponibilità** delle informazioni alle parti interessate;
- **minimizzare l'impatto in caso di incident** relativo alla sicurezza delle informazioni;
- **garantire la continuità dei servizi** secondo quanto definito dalle normative vigenti e dagli SLA contrattuali;
- **migliorare in modo continuo la sicurezza delle informazioni** contemperando l'evolversi continuo degli aspetti tecnologici.

La politica è condivisa con le parti interessate dalla Direzione Generale del SGSI e dai Managers delle aree afferenti al contesto oggetto di certificazione.

TESISQUARE® ha definito gli obiettivi per la sicurezza delle informazioni che vengono aggiornati in occasione del Riesame della Direzione o quando ritenuto necessario dalla Direzione SGSI.

TESISQUARE®, in linea con le esigenze delle parti interessate, eroga servizi assicurando adeguati livelli di sicurezza e minimizzando i rischi derivanti dalle minacce alla sicurezza delle informazioni.

Inoltre TESISQUARE® si impegna ad un costante miglioramento del SGSI, tenendo conto di:

- **Strategie di business** – Le strategie di business sono definite considerando le esigenze di mercato, la legislazione vigente, la contrattualistica, le direttive e i regolamenti di riferimento;
- **Impatto ambientale e cambiamento climatico** – Nella gestione del Sistema per la Sicurezza delle Informazioni, vengono adottate misure per il contenimento degli impatti sul cambiamento climatico; Le conseguenze dei cambiamenti climatici, come eventi atmosferici estremi o interruzioni prolungate dei servizi essenziali, possono influire significativamente sulla capacità operativa delle organizzazioni, esponendo i sistemi informativi a potenziali vulnerabilità in termini di Disponibilità, Integrità e Riservatezza dei dati. Per questo, tali scenari di rischio vengono considerati nell'analisi d'impatto sulla Sicurezza delle informazioni.
- **Scenari di rischio attuali e futuri** – Gli scenari di rischio sono sottoposti a valutazione preventiva rispetto alle riunioni di Riesame della Direzione per determinare la coerenza delle contromisure in atto con l'evoluzione e le esigenze di mercato;
- **Ruoli e responsabilità definite** – I ruoli, le responsabilità e le autorità per il personale del SGSI sono definite e comunicate ai collaboratori per mezzo di comunicazioni e documenti;
- **Programmi di formazione e/o informazione** – Tutti i collaboratori che operano nelle aree del contesto oggetto di certificazione vengono formati e periodicamente aggiornati per mezzo di training specifici e/o disposizioni organizzative anche per far fronte alle nuove esigenze normative;
- **Programmi di audit** – Il SGSI è sottoposto ad audit periodici che ne assicurano l'efficacia e la conformità.

Il management di TESISQUARE® si impegna a:

- riesaminare periodicamente la presente Politica per la Sicurezza delle Informazioni;
- mantenere la Politica coerente al modello di business e all'organizzazione aziendale;
- orientare le proprie scelte strategiche al fine di ottenere un miglioramento continuo;
- mettere a disposizione adeguate risorse per il raggiungimento degli obiettivi del SGSI.

La Direzione SGSI
Guido Ferrero
Massimo Crivello
Gianluca Giaccardi