La politica per la Sicurezza delle Informazioni
ISO / IEC 27001:2022

La politica per la sicurezza per le risorse incluse nel SGSI è quella di proteggere tali risorse dalle minacce (interne, esterne, deliberate, accidentali) che possono comprometterle, garantendo primariamente che la Riservatezza, l'integrità e la Disponibilità delle informazioni.

In particolare, per tutti i sistemi sotto SGSI, l'organizzazione si impegna affinché:

- Le informazioni siano accessibili esclusivamente alle persone autorizzate, sia interne che esterne all'azienda, garantendo livelli di servizio e complessità compatibili con i requisiti funzionali dei sistemi interessati;
- Qualunque sia il formato delle informazioni trattate, sia garantita la loro disponibilità, integrità e riservatezza nel rispetto dei requisiti legislativi 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 e forum per la pronta individuazione di nuove tipologie di minacce;
- Sia prestata particolare attenzione alle variazioni dei requisiti normativi, contrattuali ed alle relative priorità in relazione a nuovi sviluppi applicativi;
- Sia garantita la continuità operativa attraverso interventi mirati, sia organizzativi che tecnologici, e che tali interventi siano definiti, costantemente aggiornati e periodicamente verificati;
- Tutto il personale sia addestrato sulla sicurezza, che sia informato dell'obbligatorietà delle politiche aziendali in merito e che sia altresì sensibilizzato sulle conseguenze derivanti dalla violazione delle politiche aziendali;
- Siano effettuate valutazioni periodiche dell'efficacia del SGSI e della formazione del personale attraverso simulazioni nell'ambito di applicazione (vulnerability assessment, penetration test, test di conoscenza delle policy e simulazioni di violazioni delle stesse);
- Siano introdotte metriche per la valutazione delle prestazioni del sistema;
- Siano separate le mansioni relative alle attività critiche (ad esempio sviluppo e collaudo con la produzione);
- 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 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 del SGSI relativamente a:
    - verifica dell'attualità e dell'efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi;
    - incidenza dei controlli attuati sull'efficacia gestionale;
    - modifiche apportate dalla tecnologica (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico);
    - modifiche apportate alla configurazione dei sistemi sotto SGSI;
    - rivalutazione periodica del rischio ed in particolare a monte e a valle di qualsiasi azione preventiva.

Viene inoltre definita la metodologia di valutazione del rischio basata sulle linee guida della ISO/IEC 27005 ed sono individuati gli obiettivi e relativi parametri di monitoraggio per la gestione delle performance del sistema.
Gli obiettivi sono descritti nel documento ISMS_Obiettivi di sistema.

La responsabilità dell'istituzione e della gestione del SGSI è assegnata al Responsabile della Sicurezza delle Informazioni (Security Manager)

Roma, 28.05.2024