Milano, 24 marzo 2022

Oggetto: Politica del sistema di gestione

Il Sistema di Gestione della Sicurezza delle Informazioni ha come obiettivo primario la protezione del patrimonio informativo di SupplHi e il mantenimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni.

Il raggiungimento di adeguati livelli di sicurezza consente all'azienda di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone, sull'immagine e la reputazione aziendali, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni.

In tale ambito, l'Azienda individua i seguenti obiettivi per il presente manuale:

- Adottare e implementare principi e *best practice* riconosciuti per garantire la Sicurezza delle Informazioni e promuovere l'acquisizione di certificazioni di conformità agli standard di riferimento;
- Individuare ruoli e responsabilità da assegnarsi al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave qualora presenti;
- Assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la sicurezza fisica, logica ed organizzativa;
- Individuare, documentare e applicare regole che disciplinano le modalità di utilizzo delle informazioni, dei beni e degli strumenti;
- Sviluppare un programma di consapevolezza per il personale, mediante sessioni informative e formative periodiche;
- Predisporre adeguate misure di reazione e gestione a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività;
- Impegnarsi a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione per la Sicurezza delle Informazioni, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere il patrimonio informativo aziendale

La sicurezza viene vista come un insieme di processi ciclici a ogni livello e lo standard ISO/IEC 27001:2013 si concentra su aspetti di gestione della sicurezza, definendo un catalogo di contromisure di sicurezza ad un livello tale che possano essere applicate ad ambienti, sistemi e procedure diverse all'interno di qualsiasi tipo di azienda.

L'Azienda, inoltre, ha deciso di estendere il proprio SGSI alla ISO/IEC 27017 e ISO/IEC 27018 per quanto concerne la protezione delle informazioni nel Cloud. L'esigenza nasce dalla necessità di rispondere alle molteplici richieste provenienti dall'esterno e dall'interno dell'organizzazione, inclusa la necessità di rispondere a quanto definito dal GDPR in materia di protezione dei dati personali di clienti e dipendenti.

I passi principali per gestire la sicurezza delle informazioni secondo la norma possono essere efficacemente riassunti tramite il paradigma ciclico PDCA (Plan, Do, Check, Act).