

La Sicurezza delle Informazioni si ottiene applicando un complesso set di controlli indicati dalla norma ISO/IEC 27001 ed impostando con costanza ed efficacia Politiche, Processi, Procedure, Strutture organizzative, Funzionalità hardware e software ed un costante monitoraggio per il miglioramento continuo.

Pertanto la sicurezza delle informazioni è una responsabilità gestionale, e non un fattore esclusivamente tecnologico. Con questa convinzione accompagnata dalla esigenza costante di ricerca di nuove strategie di mercato volte a dare garanzie, non soltanto sulla qualità dei servizi erogati, ma anche sulle modalità di trattamento delle informazioni riguardanti clienti, fornitori e altre parti interessate, oltre che della propria struttura organizzativa, RES ha deciso l'implementazione del SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) modellato sulla base dello standard ISO 27001.

Il SGSI attualmente copre, analogamente all'integrato e gemello SQ ex UNI EN ISO 9001 2015 le attività erogate nel campo della progettazione, sviluppo ed erogazione di prodotti e consulenze in ambito software/IT per la gestione e il governo di sistemi informativi complessi.

Infatti RES in questa ottica ambisce a conseguire e mantenere il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza connessi ai servizi erogati, si prefigge la finalità di proteggere da tutte le minacce - interne o esterne, intenzionali o accidentali - il patrimonio informativo aziendale, ivi comprese le informazioni e i dati relativi a clienti e fornitori; inoltre si prefigge la finalità di mantenere e dimostrare la correttezza delle trattative con clienti e fornitori e di dare evidenza che i servizi erogati non causino direttamente un aumento dei rischi per i clienti.

Per il perseguimento di tali finalità, RES ha individuato nella documentazione del Sistema di Gestione per la Sicurezza delle Informazioni le modalità di valutazione e i criteri di gestione dei rischi, valutando gli investimenti economici che l'implementazione e il mantenimento del Sistema di Gestione potrà comportare.

Pertanto, RES si impegna, nel rispetto dei requisiti cogenti ad assicurare che:

- le informazioni siano protette da accessi non autorizzati, anche ricorrendo alla crittografia di dati e comunicazioni, nel rispetto della riservatezza e siano disponibili agli utenti autorizzati quando ne hanno bisogno, essendo questo un aspetto cardine dell'attuale perimetro del SGSI;
- le informazioni non vengano rivelate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;

- vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- il Personale riceva addestramento e aggiornamento sulla sicurezza delle informazioni.;
- tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati.

Attraverso l'attuazione di questa politica RES intende ottemperare all'impegno di conformità a UNI CEI ISO/IEC 27001:2013 nonché di conseguire e mantenere tale certificazione. Per il conseguimento di tale obiettivo, la direzione di RES si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da stagisti, collaboratori esterni, consulenti, fornitori sotto contratto, con particolare attenzione agli outsourcer che siano in qualsiasi modo coinvolti con le informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni.

La direzione di RES si impegna infine a riesaminare regolarmente la politica ed eventuali modifiche che la influenzino, per accertarsi che permanga idonea all'attività e alla capacità di aziendale di soddisfare i Clienti, i Fornitori e le altre parti interessate.