STANDARD ISO ISO/IEC 27001

Lo **standard ISO 27001** è uno degli strumenti più efficaci per garantire il controllo della sicurezza dei dati e la loro protezione in azienda.

Partendo dalla valutazione dei rischi e dalle criticità legate al sistema di gestione, la **certificazione ISO 27001:2017** permette di sviluppare ed integrare efficacemente tutti i controlli necessari ad avere un livello di sicurezza efficiente e conforme alle norme contenute nel Regolamento privacy.

Ottenere la certificazione 27001:17 da parte di un Ente qualificato significa garantire che il livello di sicurezza dei dati dell'Organizzazione è conforme ai requisiti imposti dalla legge, che l'Azienda tiene alla protezione delle sue informazioni e che attua tutte le procedure e i controlli necessari.

MODI® eroga servizi di consulenza aziendale per l'implementazione e l'assistenza post certificazione di Sistemi di Gestione conformi alle norme ISO 9001, 14001, 27001, 37001, 39001, 45001 ecc.

In particolare per chi intende valutare l'avviamento di un progetto di realizzazione di un Sistema di Gestione Sicurezza dell'Informazione (SGSI) in accordo ai criteri della norma UNI EN ISO 27001:2017, il programma di lavoro che segue interesserà in momenti diversi tutti i settori della Società. Esso è diviso nelle macrofasi che elenchiamo di seguito:

1. **Analisi iniziale:**
   viene svolta presso la Società raccogliendo tutte le informazioni che permettono di tracciare un quadro della situazione esistente, stabilire gli obiettivi nelle diverse aree ed individuare il percorso necessario per la definizione delle procedure operative. Vengono coinvolte le risorse che, all'interno dell'Organizzazione, sono in grado di fornire informazioni sui processi operativi e sulle regole che li governano;
2. **Definizione Contesto Organizzativo:**
   Presso la Società viene effettuata un'analisi che ha lo scopo di determinare i fattori esterni ed interni rilevanti per le sue finalità ed indirizzi strategici. Vengono individuate le parti interessate pertinenti per il Sistema, determinato il campo di applicazione, identificati i processi operativi e messo in atto il procedimento di *risk assessment* relativo alla sicurezza delle informazioni;
3. **Attuazione del Sistema Gestione Sicurezza dell'Informazione:**
   Durante questa fase prende corpo l'impianto documentale del Sistema di Gestione della Sicurezza dell'Informazione e, contestualmente, ne viene predisposta l'applicazione operativa. Vengono coinvolte le risorse, nei vari settori dell'Organizzazione, sia attraverso interventi formativi sull'efficace applicazione dei requisiti del SGSI, sia per l'individuazione delle migliori regole operative da attuare. Vengono affrontati tutti gli aspetti dell'attività aziendale;
4. **Audit interni e Riesame Direzione:**
   Le procedure operative, messe in atto durante la fase di attuazione del sistema, vengono verificate attraverso specifici audit interni, eseguiti con la medesima tecnica utilizzata dagli organismi di certificazione. Tali audit permettono di valutare la completezza e l'efficacia del Sistema di Gestione della Sicurezza dell'Informazione. Nel corso dell'attività di auditing, come richiesto dalla norma di riferimento, viene formato e qualificato il personale che, nell'Organizzazione, sarà preposto all'esecuzione degli audit interni. Come preparazione finale e a completamento della documentazione operativa, viene predisposto il "Riesame della Direzione" come previsto dalla norma;
5. **Assistenza in fase di certificazione:**
   Il progetto si conclude con l'affiancamento e l'assistenza al personale della Società durante l'audit per la certificazione ISO 27001 da parte dell'Organismo incaricato.

I vantaggi principali legati all'ottenimento della Certificazione ISO 27001:2017 sono:

1. strumento per l'aggiornamento continuo delle proprie infrastrutture tecniche ed organizzative;
2. compliance con le norme legislative applicabili nel settore IT e sicurezza delle informazioni, in particolar modo rispetto al GDPR UE 2016/679;
3. controllo e misurazioni dei rischi legati all'IT;
4. garanzia della sicurezza dei dati e delle informazioni aziendali (Privacy);
5. gestione migliore delle relazioni con gli stakeholders aziendali;
6. integrabilità con i principali Sistemi di gestione ISO 9001, 14001, 37001, 45001, 50001 ed un efficace utilizzo del modello PDCA (Plan, Do, Check, Act) nei processi di risk assessment;
7. offerta ai propri clienti di applicazioni sicure in termini di riservatezza, integrità e disponibilità dei dati e delle informazioni trattate;
8. riduzione dei rischi informatici e conseguente diminuzione di eventuali danni economici legati alla perdita o all'hackeraggio degli stessi;
9. sistema di sicurezza IT accettato in tutto il mondo;
10. team di lavoro più consapevole dell'importanza della sicurezza delle informazioni.