



NORMA ISO/IEC 27001:2013

Le informazioni rappresentano il patrimonio fondamentale di qualunque Organizzazione. La protezione di tale patrimonio diventa la condizione irrinunciabile per la crescita e il successo delle proprie attività. Definire ed attuare un Sistema di Gestione per la Sicurezza delle Informazioni significa salvaguardare **la riservatezza, l'integrità e la disponibilità** delle informazioni dell'Organizzazione, siano esse in formato cartaceo, elettronico, intellettuale o date in outsourcing, a prescindere dal know how degli utilizzatori. E' necessario che il sistema gestisca la sicurezza delle informazioni in modo dinamico, reagendo prontamente ed efficacemente all'insorgere di nuove minacce e vulnerabilità e migliorando costantemente le proprie prestazioni.

La **Norma ISO/IEC 27001:2013** partendo dall'analisi dei rischi applicata all'Organizzazione, o ad una parte di essa, offre gli strumenti necessari alla definizione e attuazione di un **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)**.

La Norma si concentra sugli aspetti propri della gestione della sicurezza, proponendo opportune **contromisure ("controlli")** con un livello di dettaglio tale da consentire la loro applicazione a tutte le Organizzazioni, siano esse grandi, medie o piccole con strutture IT più o meno complesse. La Norma assicura inoltre il rispetto del requisito fondamentale di qualunque sistema di gestione e cioè che non sia sufficiente implementare un insieme di controlli e procedure per la sicurezza, ma che occorra gestirli, mantenerli e migliorarli nel tempo. In altre parole un Sistema dinamico in grado di reagire prontamente ed efficacemente ai mutamenti delle condizioni di lavoro interne e del "mondo esterno".

La **certificazione** di un Sistema di Gestione per la Sicurezza delle Informazioni **garantisce il controllo dei vari fattori legati alla tutela delle informazioni**, per quanto riguarda gli aspetti tecnologici, operativi, procedurali, umani, ambientali e **consente di valorizzare gli investimenti intrapresi**.

La FQF opera ad oggi come una delle prime società che sono in grado di dare adeguata consulenza per giungere alla certificazione secondo la **Norma ISO/IEC 27001:2013**. I professionisti della FQF hanno frequentato e superato un corso di 40 ore per valutatori di Sistemi di Gestione per la Sicurezza delle Informazioni/*itc security auditor* ISO 27001, sono di elevata competenza nel settore dell'ITC, della Security e nella normativa cogente applicabile, hanno profonde competenze organizzative e strumentali per la gestione del processo di tutela dell'operatività e dei dati aziendali.

La consulenza dei professionisti della FQF, basata sullo standard ISO/IEC 27001 e ISO 17799, si rivolge a tutte le società per le quali le informazioni rappresentano un valore

NORMA ISO/IEC 27001:2013

strategico e/o sono parte integrante dell'offerta di prodotti/servizi: tra queste le aziende del settore bancario ed assicurativo, le Pubbliche Amministrazioni, le aziende che operano nel settore sanitario, le società di outsourcing di servizi informatici e, in generale, tutte le aziende che intendono tutelare il proprio know-how tecnologico e commerciale.

La consulenza dei professionisti della FQF darà un supporto al Management alle scelte dell'Organizzazione in materia di sicurezza delle informazioni e di organizzare, coerentemente con le disposizioni della legislazione italiana e con gli strumenti messi a disposizione dalla normativa di settore, tutte le azioni di tutela e salvaguardia del patrimonio informativo aziendale.

I "passi" principali per la definizione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sono:

Stabilire in modo preciso l'ambito, i confini e le interfacce;

Stabilire le Politiche e gli obiettivi;

Identificare i rischi scegliendo un'adeguata metodologia per l'analisi del rischio;

Analizzare e valutare i rischi, identificando le azioni per il loro trattamento;

Selezionare le opportune contromisure ("controlli") tra quelli suggeriti dalla Norma;

Sottoporre i rischi residui al Management per la loro accettazione;

Sottoporre il SGSI al Management per approvare la sua attuazione.

I "passi" per la certificazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sono:

Pre-Audit (facoltativo): una visita preliminare per la verifica dello stato di applicazione del SGSI;

Visita di Stage 1: verifica della documentazione del SGSI e dello stato di applicazione;

Visita di Stage 2 (Certificazione): verifica dell'implementazione del SGSI;

Approvazione: gli Organismi Tecnici di Controllo dell'Ente Terzo scelto per la verifica di certificazione effettuano l'esame dei rapporti di visita ed autorizzano il rilascio del certificato;

Rilascio del certificato ed invio all'Azienda.

Per il mantenimento della certificazione sono previste verifiche periodiche a cadenza almeno annuale.

La certificazione in accordo alla Norma ISO/IEC 27001:2013 offre alle Organizzazioni benefici diretti e concreti:

salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni;

influenza positiva sul prestigio aziendale, sull'immagine, sui parametri di *goodwill* esterna fino ad una possibile incidenza sulla valutazione patrimoniale;

valorizzazione degli investimenti e rafforzamento dell'immagine aziendale;

segnale forte verso un mercato sempre più sensibile alla problematica sicurezza;

fattore di vitalità per il sistema di gestione stesso, migliorandone efficienza/efficacia e rispondenza ai requisiti legali e contrattuali;

strumento di supporto verso enti regolamentatori ed autorizzatori.