FOCUS SICUREZZA INFORMAZIONI

ISO 27001:2013 – SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Nel quadro della crescente importanza dei sistemi di comunicazione, dello scambio di dati e della problematica relativa alla tutela dei dati, gli interventi volti alla sicurezza delle informazioni assumono un'importanza sempre maggiore nella vita delle imprese. Le informazioni custodite con mezzi informatici rappresentano buona parte del capitale intellettuale di un'azienda: sono uno strumento strategico per lo sviluppo e la tutela dell'organizzazione.

Dal punto di vista dell'impresa non basta più la sola tecnologia per la difesa delle informazioni stesse: bisogna affiancarla ad una strategia organizzativa, ad un set di procedure specifiche per renderla una fase attiva della vita aziendale.

Un processo che contribuisce alla creazione di valore ed implica lo sviluppo e l'applicazione di policy aziendali e di procedure per possibili situazioni di rischio, permettendo così un adeguato controllo della sicurezza e una difesa da possibili minacce.

Un **Sistema di Gestione di Sicurezza delle Informazioni** (SGSI) conforme allo standard ISO/IEC 27001:2013 è lo strumento, internazionalmente riconosciuto, attraverso il quale un'organizzazione può dimostrare di essere capace di **tutelare in modo globale il proprio patrimonio informativo** (o quello di terzi a lei affidato).

Lo standard consente l'identificazione e l'**aggiornamento costante dei processi** riguardanti il controllo della sicurezza fisica, logica ed organizzativa; l'analisi dei rischi per l'identificazione delle misure idonee di sicurezza; la gestione di opportune procedure e istruzioni operative frequentemente aggiornate; il monitoraggio dei processi aziendali.

La norma ISO/IEC 27001 è l'unica norma internazionale soggetta a verifica e certificabile che definisce i requisiti per un SGSI ed è progettata per garantire la selezione di controlli di sicurezza adeguati e proporzionati. In questo modo **è possibile proteggere le informazioni dai rischi interni ed esterni, dare fiducia agli stakeholders**, in particolare ai propri clienti.

Obiettivi

La norma ISO/IEC ISO 27001 mira a garantire:

- la **riservatezza**: proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati;
- l'**integrità**: proprietà relativa alla salvaguardia dell'accuratezza e della completezza delle informazioni e dei beni ad esse collegati;
- la **disponibilità**: proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

Caratteristiche

Il Sistema di gestione della Sicurezza delle informazione è caratterizzato da, e prende in considerazione:

- le **persone**, le quali devono essere consapevoli del loro ruolo al fine di garantire la sicurezza delle informazioni;
- i **processi**, che devono essere conosciuti, mappati e analizzati in termini di opportunità e rischi;
- le **tecnologie**, che devono essere gestite e mantenute.

La norma adotta un **approccio di processo** per costituire, attuare, applicare, controllare, riesaminare, gestire e migliorare un Sistema di Gestione della Sicurezza delle Informazioni.

La norma ISO 27001 viene applicata secondo il noto modello PDCA (Plan, Do, Check, Act) che consente di adottare un sistema di gestione con metodologie tali da garantire:

- la pianificazione (PLAN = dire ciò che si fa);
- la realizzazione (DO = fare ciò che si è detto);
- il controllo e la misurazione (CHECK = registrare ciò che si è fatto);
- il riesame per il miglioramento continuo e l'applicazione delle migliorie individuate (ACT = verificare e mettere a sistema).

Il tutto per un rafforzamento della leadership e della consapevolezza dei ruoli che ogni parte dell'organizzazione è chiamata a svolgere. Ognuno parte proattiva di un tutto.

Ciò consente all'azienda di:

- attuare sistematicamente la politica di sicurezza informazioni;
- applicare una gestione globale dei rischi legati alla sicurezza delle informazioni e sistemi corrispondenti;
- attuare un monitoraggio efficace dei settori a rischio;
- definire ed attuare idonei obiettivi ed interventi di sicurezza;
- rispettare i principi legislativi e contrattuali;
- attuare metodiche generali (tecniche, come ad esempio Vulnerability assessment, test penetration ed organizzative);
- eseguire un'analisi sistematica dei rischi;
- dare garanzie a se stessa e ai terzi.

Per implementare il Sistema di Gestione della Sicurezza delle Informazioni **di norma** si approccia un modello che **consente di analizzare i molteplici aspetti (di business, tecnologici e strutturali) dell'organizzazione.** Tale modello ripercorre gli aspetti richiesti dalla norma ISO 27001 **in modo esaustivo e coerente con le esigenze dell'organizzazione**. Le fasi sono le seguenti:

Impostazione del progetto	Questa prima fase prevede l'impostazione del progetto di implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI). La pianificazione permette all'organizzazione di **comprendere l'entità e le criticità del sistema di gestione in oggetto e di definire le priorità, i tempi, i ruoli e le responsabilità**.
Definizione del campo di applicazione e delle politiche di sicurezza	La definizione della politica del SGSI e la **definizione dettagliata del campo di applicazione** con il relativo perimetro fisico e logico, sono i principali fattori per ottenere una efficace implementazione del sistema di gestione. In particolare nella definizione del campo di applicazione vengono considerate le **informazioni critiche gestite dall'organizzazione**.
Analisi dell'organizzazione e dei suoi processi	L'analisi della stato attuale dell'organizzazione consente di individuare i **requisiti contrattuali e normativi e le risorse informative** da prendere in considerazione.
Conduzione dell'analisi dei rischi con focus sulle problematiche per garantire la continuità operativa	Questa fase prevede **l'identificazione, l'analisi, la valutazione e la pianificazione del trattamento dei rischi e la selezione delle contromisure rilevanti** coerentemente con le linee guida riportate dalle norme ISO/IEC 27005:11 – ISO 31000:2009. Tale analisi viene svolta sulla base degli obiettivi strategici, della politica e del campo di applicazione definiti e delle risorse informative coinvolte.
L'implementazione del sistema di gestione delle sicurezza delle informazioni	Questa fase prevede l'implementazione del Sistema di gestione della sicurezza delle informazioni attraverso le attività di **formazione continua**, **monitoraggio, misurazione audit interni, formazione e consapevolezza, gestione incidenti, riesami della direzione, miglioramento del sistema.**