UNI EN ISO 27001
Sistema di gestione per la sicurezza delle informazioni

Nello scenario della crescente importanza della rete nei sistemi di comunicazione, dello scambio di dati ad essa correlato e della problematica relativa alla tutela dei dati, le azioni finalizzate alla sicurezza delle informazioni assumono oggi un'importanza strategica nella vita delle imprese.

Il numero di attacchi, virus e intrusioni cui si deve far fronte quotidianamente testimonia l'importanza di salvaguardare le informazioni gestite dai propri sistemi informativi in quanto patrimonio aziendale.

La sola tecnologia per la difesa delle Informazioni stesse non è più sufficiente: le aziende devono affiancare delle procedure specifiche per renderla una fase proattiva della vita dell'azienda.

ISO 27001 Di cosa si tratta?

Le Organizzazioni possono proteggersi da potenziali minacce alla sicurezza delle informazioni da esse gestite sviluppando un Sistema di Gestione per la Sicurezza delle Informazioni, conformemente a quanto definito dalla ISO 27001, standard internazionale che raccoglie le best practices inerenti alle misure di gestione della sicurezza, con lo scopo di proteggere le informazioni dell'azienda e garantire la protezione dei dati dei clienti.

La certificazione secondo la norma ISO 27001 è applicabile a tutte le Organizzazioni, di qualsiasi dimensione e operanti in qualsiasi settore, con particolare focus ai settori commerciali e industriali (automotive), nonché alle pubbliche amministrazioni, e dimostra che è stato fatto quanto necessario per minimizzare i rischi a cui sono sottoposte le informazioni gestite (accesso non autorizzato, distruzione e furto dati, interruzione di servizio, virus informatici, ecc.).

Avere un corretto sistema di gestione della sicurezza delle informazioni significa dotarsi di tutte le misure di sicurezza, assicurando i dati in termini di:

- Riservatezza – proteggere le informazioni da accessi non autorizzati
- Integrità – salvaguardare l'accuratezza e la completezza delle Informazioni
- Disponibilità – assicurarsi che i dati e le informazioni siano accessibili quando richiesto.

I vantaggi della certificazione

• Rafforzare la credibilità e la visibilità dell'azienda salvaguardandone l'immagine e il patrimonio e facilitando il reperimento delle informazioni;
• Soddisfare le richieste degli Stakeholders dimostrando di affrontare e gestire il rischio e garantendo il mantenimento dei più alti standard di sicurezza delle informazioni;
• Ridurre le interruzioni dei processi critici, diminuire gli incidenti della sicurezza che comportano responsabilità legali e contrattuali e gestire i costi degli stessi;
• Migliorare le relazioni con la Pubblica Amministrazione;
• Assicurare la protezione del know-how aziendale.

Come interviene Mixa

Ti supportiamo in tutte le fasi di iter per la Certificazione:

01

Assessment iniziale

Assessment iniziale finalizzato a definire la situazione dell'azienda con particolare focus all'integrazione dell'analisi dei rischi – risk assessment sicurezza delle informazioni

02

Implementazione

Sviluppo delle azioni specifiche in termini IT, legali (requisiti previsti dal GDPR) e sviluppo del sistema di gestione

03

Audit interno e follow-up

Al fine di garantire che tutti gli elementi caratteristici siano stati aggiunti ovvero implementati per un ottimale allineamento con quanto richiesto dalla norma

04

Assistenza durante la verifica dell'ente terzo certificatore

Assistenza in fase di certificazione