La Certificazione ISO/IEC 27001

Panoramica: sicurezza delle informazioni nell'attuale contesto normativo

Le informazioni rappresentano oggi un fattore chiave di produzione e di successo per le organizzazioni moderne. La digitalizzazione, i servizi cloud, il lavoro mobile, le catene di approvvigionamento interconnesse e i crescenti requisiti normativi comportano una dipendenza sempre maggiore delle aziende dall'elaborazione sicura e dalla disponibilità delle informazioni. Allo stesso tempo, sono in aumento i rischi derivanti da attacchi informatici, violazioni dei dati, guasti dei sistemi e inadempienze normative.

In questo contesto, gli obiettivi di protezione della riservatezza, dell'integrità e della disponibilità assumono un'importanza crescente. Le informazioni costituiscono un asset aziendale di valore, e la loro perdita, manipolazione o divulgazione non autorizzata può causare danni economici, legali e reputazionali rilevanti. Oltre ai rischi operativi, stanno diventando sempre più rilevanti anche le violazioni dei requisiti legali e normativi, ad esempio in materia di protezione dei dati, sicurezza IT o normativa di vigilanza. Un sistema efficace di gestione della sicurezza delle informazioni (ISMS) rappresenta la base per affrontare queste sfide in modo strutturato.

Un ISMS consente l'identificazione, la valutazione e il trattamento sistematico dei rischi per la sicurezza delle informazioni. Inoltre, garantisce che la sicurezza delle informazioni sia integrata nell'organizzazione in modo sostenibile, trasparente e verificabile. Vengono considerati in modo equilibrato gli aspetti tecnici, organizzativi, del personale e fisici. La norma internazionale ISO/IEC 27001 definisce i requisiti per la creazione, l'integrazione, il funzionamento, il monitoraggio e il miglioramento continuo di un sistema documentato di gestione della sicurezza delle informazioni (ISMS).

Essa adotta coerentemente un approccio basato sul rischio ed è concepita per essere neutrale rispetto alla tecnologia e al settore.

La certificazione ISO/IEC 27001 da parte di TÜV NORD CERT conferma che tali requisiti sono stati attuati in modo efficace e che la sicurezza delle informazioni è parte integrante della gestione aziendale.

Caratteristiche principali della certificazione ISO/IEC 27001:

Standard riconosciuto a livello internazionale per i sistemi di gestione della sicurezza delle informazioni
Approccio olistico basato sul rischio per la gestione dei rischi di sicurezza delle informazioni
Strutture di governance chiare con ruoli e responsabilità definiti
Processo di miglioramento continuo attraverso audit, riesami e controllo delle azioni
Struttura basata sulla Harmonized Structure (HS), applicata nella maggior parte degli standard moderni di sistemi di gestione, che consente ampie sinergie con altri standard (ad esempio documentazione integrata, programmi congiunti per audit interni e riesami della direzione, e in particolare programmi di certificazione e audit integrati).

Inquadramento nel contesto normativo e della conformità:

- Supporto nel rispetto dei requisiti legali e normativi
- Dimostrazione strutturata della sicurezza delle informazioni nei confronti di clienti, partner, autorità di vigilanza e auditor
- Soddisfacimento dei requisiti contrattuali di sicurezza nelle catene di fornitura e del valore, sia nazionali che internazionali

Destinatari della certificazione:

La certificazione è rivolta a organizzazioni di tutte le dimensioni e di tutti i settori. I destinatari tipici sono organizzazioni:

- che trattano informazioni sensibili o critiche per il business (ad esempio dati personali, dati di ricerca e sviluppo, proprietà intellettuale);
- soggette a requisiti legali e normativi (ad esempio infrastrutture critiche, protezione dei dati, sicurezza IT, requisiti di vigilanza);
- a cui clienti o partner richiedono la certificazione ISO/IEC 27001 come prerequisito per la collaborazione o per la partecipazione a gare;
- che intendono rafforzare nel lungo periodo la propria resilienza informatica, affidabilità e continuità operativa;
- che desiderano costruire e dimostrare fiducia presso clienti, investitori e altri stakeholder.

La norma è adatta sia a organizzazioni che dispongono già di sistemi di gestione, sia a imprese che desiderano introdurre per la prima volta la sicurezza delle informazioni in modo strutturato e olistico.

Il tuo percorso verso la certificazione ISO 27001 in 5 fasi:

1. Preparazione
2. Audit interno
3. Fase 1 audit, incluso il processo di approvazione
4. Fase 2 audit, incluso il processo di approvazione
5. Monitoraggio, incluso il processo di approvazione

Il nostro know-how per il vostro successo

TÜV NORD Italia è un partner affidabile e riconosciuto per i servizi di verifica e certificazione sul territorio nazionale.
I nostri esperti e auditor dispongono di competenze approfondite e operano in modo stabile all'interno dell'organizzazione, garantendo indipendenza, neutralità e continuità nel rapporto con i clienti.

Il valore per le organizzazioni è concreto: gli auditor accompagnano e supportano lo sviluppo aziendale, fornendo valutazioni oggettive e contribuendo al miglioramento continuo dei sistemi di gestione.

Contatti:

TÜV NORD Italia S.r.l.

tuev-nord.it
info@tuev-nord.it

Per ulteriori informazioni: