

La norma ISO/IEC 27001:

cosa serve per implementare un sistema di gestione per la sicurezza delle informazioni e ottenere la certificazione

Sempre più spesso alle organizzazioni viene richiesta la certificazione alla norma ISO/IEC 27001 per dimostrare la propria attenzione alla sicurezza delle informazioni gestite. Questo corso, destinato al management, ai responsabili IT e ai responsabili di altri sistemi di gestione, intende presentare il testo della norma, spiegandolo con esempi tratti da casi reali ed esercizi interattivi, allo scopo di far comprendere quali siano i passi necessari alla propria organizzazione per ottenere la certificazione. Viene anche presentata la corrispondenza tra i controlli della ISO/IEC 27001 e quanto richiesto dal Regolamento UE 2016/679 sulla protezione dei dati (GDPR).



Durata

Una giornata in aula oppure due sessioni di 4 ore da remoto.



Modalità di erogazione

Il corso è erogabile sia in aula dal vivo, sia in aula virtuale.



Prerequisiti

Nessun particolare prerequisito è richiesto.



Materiale didattico

Presentazione utilizzata dal docente durante il corso.

Obiettivi

Comprendere quali siano i passi necessari alla propria organizzazione per implementare un sistema di gestione per la sicurezza delle informazioni e ottenere la certificazione ISO/IEC 27001.

Target

- Management
- Responsabili IT
- Responsabili di altri sistemi di gestione

Metodologia

Esempi tratti da casi reali ed esercizi interattivi per spiegare il testo della norma.

Docente

Il docente è un Auditor ISO 27001 con riconosciute capacità divulgative ed è membro stabile della faculty di SETA.

Lingua

Italiano

Programma

- ✓ Introduzione e compatibilità con altre norme relative a sistemi di gestione
- ✓ Scopo e campo di applicazione
- ✓ Riferimenti normativi
- ✓ Termini e definizioni
- ✓ Contesto dell'organizzazione
- ✓ Leadership, politica, ruoli, responsabilità e autorità
- ✓ Valutazione e trattamento del rischio, obiettivi e pianificazione
- ✓ Risorse, competenza, consapevolezza, comunicazione, informazioni documentate
- ✓ Attività operative
- ✓ Valutazione delle prestazioni, audit interno, riesame della direzione
- ✓ Non conformità e azioni correttive, miglioramento continuo
- ✓ Appendice A - Obiettivi di controllo e controlli di riferimento
- ✓ Corrispondenza con il Regolamento UE 2016/679 sulla protezione dei dati (GDPR)