

**Titolo**

**La Norma ISO 27001:2005: Il sistema di gestione della sicurezza informatica dei dati**

**Destinatari**

- Senior Manager, IT Manager, IT Security Manager
- Personale coinvolto nella gestione, implementazione, utilizzo di contromisure di Sicurezza IT
- Consulenti, Auditor

**Obiettivi**

- Fornire cenni sulle principali norme e criteri di sicurezza
- Fornire la conoscenza approfondita dello standard ISO/IEC 27002 e della norma ISO/IEC 27001
- Illustrare l'iter di certificazione ISO/IEC 27001 secondo lo schema CSQ-DATA
- Presentare la famiglia di norme ISO/IEC 27000 e di altri standard di supporto (es. ISO TR 13335)
- Fornire le conoscenze di base dell'Analisi di Rischio
- Estrapolare dalla norma i fattori principali che permettono una buona implementazione del proprio Sistema di Gestione della Sicurezza delle Informazioni

**Durata**

2 gg

**Modalità didattiche**

- Esposizione teorica
- Esercitazioni
- Simulazioni
- Esercitazione su PC
- Analisi filmati
- Role play
- Riprese Audio-Video
- Case study

**Risultati e benefici**

- Si acquisisce la capacità di :
- comprendere con precisione le funzionalità che deve possedere un Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
  - conoscere i requisiti obbligatori della norma
  - ispirarsi ai principali standard e criteri inerenti la sicurezza delle informazioni per l'implementazione del proprio SGSI
  - confrontarsi con i concetti di base dell'Analisi di Rischio (introduzione alla ISO/IEC 27005)

<b>Titolo</b>	<b>La Norma ISO 27001:2005: Il sistema di gestione della sicurezza informatica dei dati</b>
<b>Contenuti</b>	<p><b>Generalità</b></p> <p>Il corso, oltre a fornire una panoramica sulle principali normative e standard inerenti la sicurezza delle informazioni, esamina nel dettaglio tutti i passi necessari alle organizzazioni per l'impostazione di un Sistema di Gestione per la Sicurezza delle Informazioni. La norma ISO/IEC 27001 viene approfondita correlandola alla ISO/IEC 27002, che è la guida per la selezione delle contromisure "controls", andando ad analizzare i diversi metodi di controllo e le contromisure necessarie per fronteggiare i rischi e le minacce individuate e dando una chiara visione di tutti i particolari per la reale implementazione del sistema organizzativo (<i>Management Framework</i>) a supporto della gestione della sicurezza delle informazioni trattate dall'organizzazione.</p> <p><b>Struttura del corso</b></p> <ul style="list-style-type: none"> <li>• Introduzione ai principali criteri e standard della sicurezza delle informazioni</li> <li>• ISO/IEC 27001</li> <li>• ISO/IEC 27002</li> </ul> <p><b>Programma</b></p> <ul style="list-style-type: none"> <li>• Introduzione alla sicurezza IT</li> <li>• La ISO/IEC 27001 <ul style="list-style-type: none"> <li>- L'evoluzione</li> <li>- Lo scopo della ISO/IEC 27001</li> <li>- I fattori di successo</li> </ul> </li> <li>• La ISO/IEC 27001 <ul style="list-style-type: none"> <li>- Politiche per la sicurezza delle informazioni</li> <li>- Organizzazione della sicurezza delle informazioni</li> <li>- Gestione dei beni</li> <li>- Sicurezza delle risorse umane</li> <li>- Sicurezza fisica ed ambientale</li> <li>- Gestione delle comunicazioni delle attività</li> <li>- Controllo degli accessi</li> <li>- Acquisizione di sistemi informatici, Sviluppo e manutenzione</li> <li>- Gestione degli incidenti di sicurezza delle informazioni</li> <li>- Gestione della continuità dei processi aziendali</li> <li>- Conformità (a disposizioni di leggi ed alle Politiche di Sicurezza)</li> </ul> </li> <li>• La ISO/IEC 27002 <ul style="list-style-type: none"> <li>- L'implementazione della dichiarazione di applicabilità</li> <li>- Lo svolgimento di una certificazione La ISO/IEC 27001</li> </ul> </li> <li>• I Technical Report ISO TR 13335 (Cenni)</li> <li>• Analisi del Rischio e la ISO/IEC 27005 (Cenni)</li> </ul>