GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

OBIETTIVI

LA ISO 27001 è uno standard internazionale che definisce i requisiti per pianificare, attuare, operare, monitorare, riesaminare, mantenere e migliorare il sistema di gestione per la sicurezza delle informazioni sia delle aziende private, sia delle organizzazioni pubbliche .
La ISO 27001 definisce i requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione, fornendo buone pratiche sia per proteggere i dati da una vasta gamma di minacce, sia per assicurare la riservatezza, integrità e disponibilità degli stessi.
Il corso "gestione della sicurezza dell'informazione", con taglio pratico ed esempi aziendali, illustra i requisiti della norma e le regole per l'implementazione di un sistema di gestione efficace, in grado di assicurare la continuità dell'attività aziendale.

Il presente corso parte da una analisi dei principi base della sicurezza delle informazioni e degli strumenti IT come definiti sia negli standard internazionali come ISO27001, sia nelle direttive italiane di AgID (Agenzia Italia Digitale), calandoli poi nel contesto operativo degli Operatori d'Ufficio e dei loro Coordinatori. Il corso prosegue con la presentazione delle minacce più importanti degli ultimi anni e con le metodologie operative necessarie per ridurre il rischio ad esse associato. Esercizi operativi consentono di consolidare le conoscenze acquisite rendendole applicabili immediatamente per le persone.

CONTENUTI

INTRODUZIONE ALLA SICUREZZA DELLA INFORMAZIONE

- Cosa significa sicurezza dell'informazione e il suo legame con la sicurezza informatica
- Riconoscere il patrimonio di informazione dell'azienda
- Il concetto di rischio e la sua analisi
- Le qualità della sicurezza dei dati
- Le qualità della sicurezza dei sistemi
- Problematiche da guasti accidentali e da eventi naturali
- Le minacce umane alla sicurezza
- Accettare e gestire il rischio

PRINCIPI DEI SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

- Riservatezza e Integrità
- Disponibilità e Conformità
- Obiettivi e e struttura del sistema di gestione
- Compatibilità con le altre norme sui sistemi di gestione
- Politica per la sicurezza delle informazioni

CONTENUTO DELLA NORMA ISO 27001

- Contesto dell'organizzazione
- Ruoli e responsabilità
- Azioni per affrontare rischi e opportunità
- Obiettivi e pianificazione
- Risorse e competenze
- Comunicazione e informazioni documentate

PIANIFICAZIONE, CONTROLLO, MIGLIORAMENTO

- Pianificazione e controllo operativi
- Valutazione e trattamento del rischio
- Monitoraggio, misurazione, analisi e
- valutazione
- Non conformità e azioni correttive
- Miglioramento continuo

IL PROCESSO DI CERTIFICAZIONE

- Regolamenti ed iter di certificazione
- Gli organismi di certificazione
- Le visite di valutazione e mantenimento

METODOLOGIE ADOTTATE

Numero ore aula/FAD:	100
Numero ore stage/tirocinio:	0
Numero ore laboratorio:	200
Durata Totale:	300
Esame finale:	SI
Tipo metodologia:	Teoria – Pratica– FAD - Visite guidate

METODOLOGIA

I programmi dei nostri percorsi sono progettati e erogati con un metodo integrato, che prevede un'alternanza di metodologie didattiche di carattere cognitivo e metodologie di carattere attivo-emotivo.

La metodologia didattica di carattere cognitivo sarà centrata sul "contenuto" dell'argomento oggetto del corso, quindi lo strumento didattico sarà la lezione frontale per il trasferimento di concetti, metodologie, strumenti di analisi, strategie di intervento ed il ricorso ad aneddoti esempi e casi concreti.

L'auto-apprendimento fuori dall'aula sarà favorito dalla consegna di dispense, slides, articoli, bibliografia, e altro materiale di approfondimento on-line erogato dal docente.

La metodologia di carattere attivo-emotivo, avrà invece l'obiettivo di facilitare l'apprendimento attraverso la sperimentazione attiva, con tecniche di gestione attiva dell'aula sviluppando un forte coinvolgimento dei partecipanti attraverso discussioni, confronti in plenaria, esercitazioni pratiche, analisi dei casi, role-playing, simulazioni, studio di Case-History, teamwork, i business game, allo scopo di verificare l'uso delle tecniche e degli strumenti proposti. Si svilupperà una forte l'interazione e una prossemica personale tra docente ed allievi.

I metodi attivi tendono ad incoraggiare una partecipazione diretta dei soggetti in formazione e favoriscono un costante feed-back all'azione del formatore.

STRUMENTI FORMATIVI E MATERIALE DIDATTICO

Carattere distintivo dei nostri percorsi formativi è l'utilizzo di strumenti dall'elevato valore formativo

che consentono di vivere in aula una esperienza sul campo simulata (Learnig by Doing):

- Case History analisys (Analisi di casi reali aziendali)
- Simulazioni What
- Esercitazioni di Business game (gestione di casi aziendali; presa di decisioni strategiche e operative;
- Filmati coerenti con l'argomento
- Project work
- Discussioni di gruppo
- Role Playing in un contesto individuale e collaborativo (team work).
- Per quanto riguarda i concetti, le teorie e le argomentazioni, sono consegnate:
- Dispense
- Slides in Power Point
- Documentazione e Articoli di approfondimento

VERIFICHE

Al fine di effettuare verifiche dell'apprendimento sono utilizzate questionari con domande chiuse, aperte, miste, a scelta multipla, esercitazioni, creazione di procedure, project work. La valutazione dell'apprendimento riguarderà contenuti, concetti, metodologie, comportamenti, abilità, ect, relativi all'argomento trattato.

DURATA

6 MES1 – 300 ORE

ATTESTATO/CERTIFICAZIONE

ATTESTATO DI FREQUENZA