

COME IMPLEMENTARE UN SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI [SGSI] CONFORME ALLA NORMA ISO/IEC 27001

codice SW12

L'AICQ Tosco Ligure in collaborazione con il Comitato Software e Servizi ICT dell'AICQ ha il piacere di presentare il seguente corso di formazione sull'Implementazione di un Sistema di Sicurezza delle Informazioni (SGSI).

Contenuti: Lo sviluppo pervasivo delle Tecnologie dell'Informazione e della Comunicazione (ICT) nella gestione aziendale pone l'esigenza per le organizzazioni di dotarsi di un Sistema di Gestione per la Sicurezza delle Informazioni in modo da proteggere il valore delle Informazioni come strumento vitale e/o fine ultimo della dinamica gestionale. Il sistema di protezione delle informazioni è tanto più efficace quanto meglio garantisce un adeguato livello di riservatezza, integrità e disponibilità. Nelle organizzazioni sta aumentando la consapevolezza sulla stretta relazione che lega il valore trasferito ai propri portatori d'interesse al valore del patrimonio delle informazioni gestite. Le norme della famiglia ISO/IEC 27k (27001, 27002 e 27003) offrono sia un approccio sistematico all'implementazione di un efficace sistema di protezione sia la garanzia di un processo di certificazione.

Destinatari: Il corso si rivolge a tutti coloro che in ruoli diversi (Imprenditori, Manager, Responsabili della Sicurezza delle Informazioni, Responsabili Qualità, ecc.) operano o intendono operare con le ICT nel trattamento dei dati relativi ai rispettivi campi della gestione. Il corso è propedeutico al corso per Auditor di verifiche ispettive sui Sistemi di Gestione della Sicurezza delle Informazioni.

Obiettivi: Il corso è finalizzato a fornire le conoscenze su SGSI, sull'interpretazione e corretta applicazione della norma ISO/IEC 27001, sulla progettazione documentazione e attuazione del Sistema secondo le linee guida ISO/IEC 27003.


Prerequisiti: buona conoscenza dei requisiti della sicurezza delle informazioni secondo la norma ISO/IEC 27001 e le altre norme della famiglia ISO27k. Conoscenza di base del sistema di gestione per la qualità e degli altri sistemi di gestione da integrare con SGSI. È consigliata la frequenza al Modulo SW11 "Introduzione ai Sistemi di Gestione della Sicurezza Informatica. La Norma ISO/IEC 27001".

PROGRAMMA

I Giornata		II Giornata		III Giornata	
09,00	Registrazione partecipanti. Presentazione del corso e delle iniziative AICQ-M	09,00	Registrazione partecipanti	09,00	Registrazione partecipanti
09,15	Evoluzione normativa in materia di gestione della Sicurezza delle Informazioni. Approccio al progetto d'implementazione del sistema sicurezza - collegamenti ed integrazioni con altri sistemi di gestione aziendale	09,15	La gestione del rischio. Metodi standard e procedure. Il rischio nella fase di Plan. Valutazione del rischio: identificazione, analisi/stima e ponderazione - risk register	09,15	La progettazione dell'organizzazione per le operazioni di esercizio del SGSI. Disegno di dettaglio dei controlli di sicurezza - organizzativa, logica e fisica. DO: Attuazione e conduzione SGSI
11,00	Intervallo	11,00	Intervallo	11,00	Intervallo
11,15	Concettualizzazione e pianificazione del progetto - definizione dei documenti di sistema. Il ciclo PDCA - la fase di Plan - definizione di ambito, perimetro e politica.	11,15	Esercitazioni - sviluppo del risk register	11,15	Esercitazioni - politiche di settore (EMAIL)
13,00	Colazione di lavoro	13,00	Colazione di lavoro	13,00	Colazione di lavoro
14,00	L'analisi dei requisiti e degli obblighi di sicurezza	14,00	Il rischio nella fase di Do. Trattamento del rischio. Definizione e pianificazione delle attività di trattamento. Il rischio nella fase di Check - monitoraggio	14,00	Disegno di dettaglio dei processi di monitoraggio e verifica (CHECK). La fase di ACT: riesame e miglioramento del SGSI. Integrazione del piano d'implementazione
16,00	Intervallo	16,00	Intervallo	16,00	Intervallo
16,15	Esercitazioni - l'inventario dei beni (asset register)	16,15	Esercitazioni - aggiornamento risk register - formulazione SOA	16,15	Esercitazioni - misure per Formazione, Incidenti e Continuità
17,30	Conclusioni - Redazione questionario	17,30	Conclusioni - Redazione questionario	17,30	Conclusioni - questionario
18,00	Fine I giornata	18,00	Fine della II giornata	18,00	Fine del corso

Per motivi organizzativi e il corso si terrà se sarà raggiunto un numero minimo di almeno 5 partecipanti. La AICQ-TL si riserva la possibilità di non procedere nella erogazione del corso nel caso non si raggiunga un numero minimo di adesioni.

Il Presidente
Ing. Giovanni Fanucchi



AICQ Tosco Ligure

c/o CIPAT Via dei Pilastri 1/3 50121 Firenze
C.F. 90027270504 - P. IVA 01521540508
Fax +39 055 0114380 Cell. Segreteria 3499150212

E-mail: aicq-tl@aicq.it Web: <http://toscoligure.aicqna.it/>

Coordinate per il bonifico bancario: Associazione Italiana Cultura Qualità Tosco Ligure
Banca: CARIPARMA **IBAN:** **IT20 L062 3002 8070 0005 6724 759**