



## **CORSO DI FORMAZIONE PER AUDITOR DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI (40 ore)**

### **PRESENTAZIONE**

Il corso è organizzato e gestito dall'Associazione Italiana Cultura Qualità Tosco-Ligure, per rispondere alla domanda di formazione ed addestramento sulle metodologie di esecuzione degli audit secondo la norma UNI EN ISO 19011:2012 e ISO/IEC 17021:2011, applicata alla valutazione e sorveglianza dei Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI) realizzati in conformità ai requisiti della norma ISO/IEC 27001:2013 utilizzando le linee guida espresse nella famiglia 27k.

Il corso è tenuto da Docenti universitari, Dirigenti di azienda e Auditor professionisti iscritti al registro AICQ-SICEV, consentendo in questo modo di associare alla professionalità dei docenti AICQ, anche l'esperienza degli Auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni professionisti. Il corso è riconosciuto da AICQ-SICEV ed il superamento dell'esame finale consente l'ammissione agli esami per l'iscrizione al registro SAFEINFO di SICEV Auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni.

Il corso è d'interesse per:

- Le persone che si propongono di sviluppare, aggiornare, certificare la propria professionalità di Auditor SGSI;
- Le persone (Consulenti e Responsabili di Sistema) o le organizzazioni che intendono stabilire, attuare, mantenere e migliorare in modo continuo un Sistema di Gestione per la Sicurezza delle Informazioni o che intendono utilizzare lo strumento degli Audit come mezzo di verifica dell'efficacia del proprio SGSI o di selezione, valutazione e sorveglianza dei propri fornitori.

### **OBIETTIVI**

Obiettivo generale del corso è preparare i partecipanti a svolgere Audit secondo le indicazioni fissate dalla norma UNI EN ISO 19011:2012 e ISO/IEC17021:2011, avendo come riferimento la norma UNI EN ISO 27001.

Perciò il corso è strutturato per:

- Fornire ai partecipanti le conoscenze di base sulla gestione degli Audit secondo la normativa indicata, impegnando gli allievi nella pratica soluzione di casi di studio, così da fare familiarizzare i partecipanti con le modalità di pianificazione, di conduzione degli audit e di presentazione dei risultati alla direzione dell'organizzazione sottoposta a audit;
- Fornire richiami sulle regole di comportamento dell'Auditor ed elementi su come migliorare le tecniche di comunicazione con i principali interlocutori.

### **PREREQUISITI**

Per un migliore apprendimento dei contenuti sotto descritti il partecipante al corso dovrebbe avere sufficienti conoscenze ed esperienze; in particolare:

- ❖ CONOSCENZE
  - Sistemi informativi
  - Sistemi di gestione aziendale
  - Sistemi di Gestione per la Sicurezza delle Informazioni
  - Famiglia di norme 27k.
- ❖ ESPERIENZE
  - Sviluppo software
  - Erogazione di servizi IT
  - Conduzione di Sistemi di gestione aziendale.

### **STRUTTURA E CONTENUTI**

Il corso è stato completamente rinnovato per renderlo più pratico e per ristrutturarlo in due moduli:

- **Il modulo A** (della durata di due giorni) è dedicato alla presentazione di:
  - Concetti generali sulla Sicurezza delle Informazioni ed i relativi Sistemi di Gestione, richiami sui requisiti espressi nella Norma UNI EN ISO 27001:2013 per la certificazione SGSI, Quadro normativo e Famiglia 27K, illustrazione di vari aspetti pratici ed esempi di applicazioni di questa norma in vari contesti;

- Obiettivi e controlli di sicurezza (ANNEX A), Processo di Audit (ISO/IEC17021:2011, UNI EN ISO 19011:2012), Gestione rischi, Esercitazioni e casi di studio con illustrazione delle modalità di programmazione pianificazione ed esecuzione degli audit, di gestione e qualificazione degli auditor, con discussione di un caso pratico.
- **Il modulo B** (della durata di tre giorni) è interamente dedicato all'applicazione pratica delle modalità di pianificazione, esecuzione e presentazione dei risultati degli audit. Le esercitazioni sono basate sullo studio di casi da parte dei partecipanti organizzati in gruppi di lavoro. I casi consistono nell'analisi della descrizione di porzioni di un audit che includono sia deficienze nell'impostazione e realizzazione SGSI, sia carenze di comportamento da parte degli Auditor. Le Non Conformità, le osservazioni e i contenuti del rapporto finale di Audit saranno discussi collegialmente sotto la guida dei docenti. Verrà inoltre simulata la presentazione finale dei risultati da parte di ogni gruppo di lavoro.

### ESAMI

L'esame finale avrà luogo nel pomeriggio del quinto e ultimo giorno di corso e mira ad accertare il livello di apprendimento degli argomenti trattati durante il corso. Esso è articolato in due prove scritte:

- la prima consiste nel rispondere in forma scritta ad un questionario che ha l'obiettivo di accertare la conoscenza applicativa delle norme illustrate.
- la seconda consiste nella valutazione di un caso di studio nel quale il candidato deve individuare e formalizzare le non conformità rispetto alla norma UNI EN ISO 27001:2013 e deve scrivere il rapporto finale di Audit.

In caso di superamento dell'esame sarà rilasciato un attestato **riconosciuto da AICQ-SICEV** ai fini dell'ammissione agli esami per la certificazione di Auditor Sistemi di Gestione per la Sicurezza delle Informazioni.

### AGENDA DEL CORSO

| Modulo A   |  | Modulo B  |  |  |
|--|--|---|--|--|
| 1° giorno  | 2° giorno  | 3° giorno   | 4° giorno  | 5° giorno  |
| Introduzione, Concetti generali sulla Sicurezza delle Informazioni ed i relativi Sistemi di Gestione, Quadro normativo e Famiglia 27K, iter di certificazione di un SGSI, Modello di riferimento SG, Requisiti UNI EN ISO 27001:2013 per la certificazione SGSI. | Obiettivi e controlli di sicurezza (ANNEX A). Processo di Audit (ISO/IEC 17021, UNI EN ISO 19011). Esempi applicativi di riferimento: Programma di audit, Piano di audit, Rapporto di audit. Competenze degli Auditor: Comunicazione interpersonale e comportamento dell'Auditor. Costituzione dei gruppi di lavoro e avvio dell'esercizio n°1 sulla verifica documentale. | Completamento dell'esercizio n°1 e discussione dei risultati. Analisi e Valutazione dei rischi. Esercizio n°2: Presentazione caso di studio su una verifica in campo, organizzazione lavoro di gruppo sul caso, identificazione delle Non Conformità, scrittura dei rapporti di NC e scrittura del rapporto finale. | Completamento esercizio n°2 e discussione dei risultati. Ripasso e approfondimento dei requisiti ISO/IEC 27001. La comunicazione. Esercizio n. 3: In analogia con l'esercizio n°2 organizzazione del lavoro di gruppo su un caso di studio concernente una verifica in campo - identificazione delle Non Conformità, scrittura dei rapporti di NC e scrittura del rapporto finale. | MATTINA: <ul style="list-style-type: none"> <li>▪ Completamento esercizio n°3 e discussione dei risultati.</li> <li>▪ Simulazione riunione finale di audit</li> </ul> POMERIGGIO dedicato agli esami: <ul style="list-style-type: none"> <li>• Questionario di accertamento della conoscenza delle norme.</li> <li>• Valutazione di tre mini-casi nei quali individuare le NC rispetto alla norma UNI EN ISO 27001:2013 e scrittura del rapporto finale di audit.</li> </ul> |

### DURATA E FREQUENZA DEL CORSO

**Il corso ha la durata di 40 ore – suddivise in 5 giorni così organizzato:**

**Orario:** mattina ore 9.00 -13.00 pausa pranzo pomeriggio ore 14,00-18,00 (salvo diversi accordi).

**Il Presidente**  
**Ing. Giovanni Fanucchi**



### AICQ Tosco Ligure

c/o CIPAT Via dei Pilastrini 1/3 50121 Firenze  
C.F. 90027270504 - P. IVA 01521540508  
Fax +39 055 0114380 Cell. Segreteria 3499150212  
E-mail: [aicq-tl@aicq.it](mailto: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