

## Preparazione alla Certificazione CISSP (Information Systems Security Professional)

La certificazione dei professionisti della sicurezza delle informazioni

 A distanza



5 giorni (35 Ore)

Open : 3.770,00 € +IVA

WebCode: IT.18

Packaged in azienda : 8.680,00 € +IVA +10% di  
Project Management (Quota riferita ad un gruppo  
di 10 pax max)

Customized : Su richiesta

La certificazione di riferimento **CISSP® (Certified Information Systems Security Professional)** è indipendente, pragmatica e riconosciuta a livello internazionale. Creata e gestita da professionisti della sicurezza informatica, consente di calibrare il proprio livello di competenza secondo **3 assi**: conoscenze **tecniche**, capacità di analisi dei **rischi** e capacità di **audit** del sistema. La certificazione CISSP non solo attesta una buona conoscenza delle tecnologie, ma dimostra soprattutto una reale capacità di intrecciarle e assemblarle per soddisfare al meglio le esigenze delle aziende in termini di sicurezza.

Questa formazione prepara alla certificazione **Certified Information Systems Security Professional (CISSP)**, che gli interessati potranno conseguire presso una struttura terza, verificando il possesso dei pre-requisiti sul sito del CISSP.

### A chi è rivolto



#### Per chi

- CISO, DSI
- Consulenti/Revisori
- Amministratori di sistema e di rete



#### Prerequisiti

- In minimo di cinque anni di esperienza professionale in almeno 2 delle 8 aree di CBK®

### Programma

#### 1 - Sicurezza delle informazioni e gestione del rischio

- I concetti di riservatezza, integrità e disponibilità
- I principi della governance della sicurezza
- Conformità
- Questioni legali e regolamentari relative alla sicurezza delle informazioni in un contesto globale
- etica professionale
- Politica di sicurezza, standard, procedure e linee guida
- requisiti di continuità operativa
- Politiche di sicurezza del personale
- Concetti di gestione del rischio
- Il modello di minaccia
- Considerazioni sui rischi per la sicurezza nella strategia di acquisizione
- Sensibilizzazione, formazione e istruzione sulla sicurezza delle informazioni

## **2 - Sicurezza patrimoniale**

- Classificazione delle informazioni e supporto delle risorse
- La manutenzione della proprietà
- Proteggere la privacy
- Garantire una corretta retention
- Misure di sicurezza dei dati
- Requisiti di gestione

## **3 - Ingegneria della sicurezza**

- Processi ingegneristici e principi di progettazione sicura
- Comprendere i concetti fondamentali dei modelli di sicurezza
- Misure e contromisure
- Le possibilità di sicurezza offerte dai sistemi informativi
- Vulnerabilità di sicurezza di architetture, design, soluzioni
- Valutare e ridurre le vulnerabilità della sicurezza nei sistemi Web, mobili e integrati
- Crittografia
- Principi di sicurezza in cantiere e nella progettazione dell'impianto
- Sicurezza fisica

## **4 - Telecomunicazioni e sicurezza delle reti**

- Principi di progettazione sicura per le architetture di rete
- Protezione dei componenti di rete
- Progettare e stabilire canali di comunicazione sicuri
- Prevenire o mitigare gli attacchi di rete

## **5 - Gestione dell'identità e degli accessi**

- Controllo degli accessi fisici e logici agli asset
- Gestire l'identificazione e l'autenticazione di persone e attrezzature
- Identità come servizio
- Servizi di identità di terze parti
- Meccanismi autorizzativi
- Attacchi al controllo degli accessi
- Il ciclo di vita del provisioning di identità e accessi

## **6 - Valutazione e collaudo della sicurezza**

- Valutazione della sicurezza e strategie di test
- Test delle misure di sicurezza
- Dati di processo di sicurezza
- Risultati del test
- Audit interni o di terze parti

## **7 - Continuità operativa e piano di risanamento**

- Indagini
- I requisiti dei tipi di indagini
- Attività di monitoraggio e registrazione
- Approvvigionamento di risorse
- Concetti di sicurezza operativa di base
- Tecniche di protezione delle risorse
- Gestione degli incidenti
- Gestire e mantenere misure di sicurezza preventive
- Gestione di patch e vulnerabilità
- Processi di gestione del cambiamento
- Strategie di recupero
- Strategie di ripristino di emergenza
- Piani di ripristino di emergenza
- Il piano di continuità operativa

- Gestione della sicurezza fisica
- Problemi di sicurezza del personale

## 8 - Sicurezza nello sviluppo di software

- Sicurezza nel ciclo di vita dello sviluppo del software
- Misure di sicurezza negli ambienti di sviluppo
- L'efficacia della sicurezza del software
- Valutare l'impatto sulla sicurezza del software acquisito



### Obiettivi del corso

- Conoscere gli argomenti, i domini e gli argomenti del Common Body of Knowledge (CBK®).
- Padroneggia i fondamenti della sicurezza IS
- Preparazione per l'esame di certificazione CISSP



### Esercitazioni

- Il contenuto della formazione viene continuamente rivisto e **aggiornato** per riflettere gli ultimi sviluppi nelle attuali questioni di sicurezza, preoccupazioni e contromisure
- La formazione è un vero e proprio luogo di **scambio** dove ogni partecipante è chiamato ad intervenire su diverse tematiche nell'ambito della CBK
- L'iscrizione all'esame non è inclusa, per superare la certificazione, ogni partecipante deve registrarsi sul sito ISC2 e inviare un file di idoneità



**Date 2026**



Ultimi posti  Edizione garantita

dal 4 mag al 12 mag

- dal 4 mag al 6 mag
- dal 11 mag al 12 mag

dal 19 ott al 27 ott

- dal 19 ott al 21 ott
- dal 26 ott al 27 ott