Innovation Training

REGIONE LAZIO

ESPERTO IN SICUREZZA INFORMATICA

- **Codice:** K1.8
- **Profilo:** Esperto in sicurezza informatica
- **Settore:** Servizi digitali
- **Corso:** *Formazione autorizzata dalla Regione Lazio (Det. N. G02495 del 26/02/2026)* con esame finale e rilascio certificato di qualifica professionale (D.lgs. 13/2013)
- **Livello EQF di qualificazione:** 6

DESCRIZIONE

L'Esperto/a in sicurezza informatica si occupa dell'analisi dei sistemi digitali hardware e software e della valutazione delle possibili vulnerabilità e rischi alla sicurezza dei sistemi. L'Esperto/a in sicurezza informatica agisce, secondo i protocolli di security by design per la gestione della sicurezza informatica. Inoltre, testa la sicurezza dei sistemi contro virus, minacce e intrusioni, - intenzionali o accidentali - la recuperabilità di dati e operazioni, a seguito di incidenti o malfunzionamenti e la corretta funzione di protezione delle informazioni, mediante opportune tecniche di crittografia. Individua soluzioni per la mitigazione dei possibili rischi, tramite opportune misure di sicurezza dei sistemi e supporta nelle attività di ripristino delle corrette funzionalità dei sistemi.

Certificato di qualificazione professionale in Esperto in sicurezza informatica rilasciato ai sensi del D.lgs. 13/2013.

DESTINATARI

Giovani e adulti con necessità di qualificazione o riqualificazione nel settore

REQUISITI OBBLIGATORI DI ACCESSO AL PERCORSO:

-essere in possesso, al minimo, di una qualificazione regionale di livello EQF 5 in ambito STEM oppure di un diploma di ITS Academy in ambito STEM oppure di un diploma di laurea triennale in ambito STEM.-essere in possesso di un livello di conoscenza della lingua inglese B1 del Quadro Comune Europeo di riferimento per le Lingue, dimostrabile tramite certificazioni linguistiche o titoli equipollenti o autodichiarazione; -(per i cittadini stranieri) essere in possesso di un livello di conoscenza della lingua italiana B2 del Quadro Comune Europeo di Riferimento per le Lingue, dimostrabile tramite certificazioni linguistiche o titoli equipollenti. Ove il candidato non disponga di attestazione di valore equivalente, è previsto lo svolgimento obbligatorio delle specifiche prove valutative in sede di selezione.

STRUTTURA DEL CORSO

Durata ore:

- 300 ore Corso Cybersecurity Technician - parte in presenza e parte in FAD
- 120 ore Tirocinio Curriculare

Durata complessiva: 420 ore

Le lezioni in aula si svolgono 3 gg a settimana tra il lunedì e il venerdì, e hanno durata da 4 o 6 ore, preferibilmente in orario pomeridiano e serale.

Un numero limitato di ore 122 di didattica potrà svolgersi in modalità FAD. Il Calendario Didattico viene fornito alla partenza.

ESAME DI QUALIFICAZIONE PROFESSIONALE

Per l'ammissione all'esame finale è necessario di aver frequentato almeno l'80% delle ore complessive del percorso formativo.

MODALITÀ DIDATTICHE

Aula didattica fino a 12 posti

PROGRAMMA DIDATTICO

Inquadramento della professione 8 ore

- Orientamento al ruolo - Elementi di diritto del lavoro, contrattualistica, regimi fiscali e responsabilità civile

Architetture di sistemi digitali 20 ore

- Architettura hardware e software dei sistemi digitali - Sistemi digitali ed ingegneria del softwar

Fondamenti di organizzazione e project management 10 ore

- Fondamenti di organizzazione aziendale - Fondamenti di project management

Quadro normativo, standard e framework in ambito cybersecurity e data quality management 30 ore

- Quadro normativo nazionale e comunitario in materia di sicurezza informatica, cybersecurity - Quadro normativo nazionale: Perimetro di Sicurezza Nazionale Cibernetica - Quadro normativo nazionale e comunitario in materia di protezione dei dati personali - Standard e framework nazionali ed internazionali in ambito cybersecurity (Security by design, Sistema di Gestione per la Sicurezza delle Informazioni – ISO 27001, Sistemi di gestione per la continuità operativa ISO 22301, NIST, Framework Nazionale per la Cybersecurity e la data protection – FNCS, NIST SP800-9 - Standard e framework di riferimento per la definizione del processo di gestione della qualità dei dati (Data Quality Management)

Analizzare le vulnerabilità software e hardware e la conformità alla normativa vigente 80 ore

- Fondamenti teorici della sicurezza dei sistemi digitali - Evoluzione ed attuale scenario delle principali vulnerabilità note - Metodologie e framework di riferimento per la misurazione vulnerabilità (es. CVSS, NVD) e conseguenti strategie di mitigazione - Metodi e strumenti per attività di Penetration Testing - Application Security tools (Static and Dynamic Application Security Testing) - Awareness, Red Teaming e Lesson Learned Techniques - Metodi di valutazione dei rischi per la sicurezza legati alle componenti hardware e software del sistema digitale - Metodi di valutazione di rischi per la sicurezza legati alle componenti del sistema digitale dedicate al networking (protocolli, connessioni, apparecchiature di rete)

Individuare processi e soluzioni a protezione del sistema digitale 64 ore

- Principali caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection - Principali caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server - Tipologie e logiche di funzionamento dei programmi informatici creati per diffondersi e sottrarre informazioni o danneggiare sistemi digitali (virus, worm, Trojan, malware, ransomware, ecc…) - Tipologie e caratteristiche degli attacchi al sistema digitale a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente - Caratteristiche e funzionalità dei firewall - Algoritmi crittografici specifici (SHA, AES, RSA, ecc.) e loro applicazione alla trasmissione sicura dei dati e alla conservazione su file system - Principali metodi e tecniche di configurazione del sistema di protezione e del firewall - Elementi di metodologie, tecniche e strumenti in ambito asset management - Autenticazione federata basata su Single Sign-On (SSO) e Identity Provider - Sistemi per la creazione e gestione di password complesse - Principali tipologie e funzionalità di un Security Operation Center - Sistemi di controllo degli accessi al sistema digitale ed alle reti: Architettura IAM (Identity

Access Management), meccanismi di autenticazione distribuita, meccanismi di Strong Authentication

Monitorare lo stato di sicurezza dei sistemi digitali 48 ore

- Principali strumenti e tecniche per l'analisi e gestione degli incidenti informatici: monitoraggio, analisi valutazione e gestione degli eventi informatici (SIEM), individuazione di anomalie - Principali metodi e tecniche per la classificazione degli eventi ed incidenti informatici (es. tassonomie nazionali/comunitarie, il framework MITRE ATT&CK™) - Principali metodi, per infrastrutture con soluzioni in locale o su cloud, e strumenti per implementare una politica di backup e restore dei sistemi digitali - Cenni sulle metodologie e strumenti per la protezione fisica dei sistemi e delle reti - Fondamenti di crisis management - Elementi sulle tecniche e infrastrutture di disaster recovery - Elementi di sistemi di gestione per la continuità aziendale (ISO 22301) - Cenni sulle metodologie e tecniche di simulazione e role playing per lo svolgimento di test e simulazioni del sistema di gestione della continuità operativa (test di DR e BC) - Cenni su metodi e tecniche per lo svolgimento di Business Impact Analysis - Principali standard e framework di riferimento in ambito gestione degli incidenti informatici - Cenni sul funzionamento e organizzazione del CERT e dei SOC e sul sistema di alert dello CSIRT nazionale - Fondamenti di organizzazione aziendale - Fondamenti di project management

Inglese tecnico 32 ore

- Inglese tecnico per l'informatica

Operare in sicurezza nel luogo di lavoro 8 ore

- Legislazione sulla salute e sicurezza sui luoghi di lavoro e applicazione delle norme di sicurezza - Gli obblighi del datore di lavoro e del lavoratore - Dispositivi di protezione individuali

Tirocinio curriculare 120 ore

Totale percorso 420 ore

SEDE DEI CORSI AUTORIZZATI

Piazza Gaspare Ambrosini, 53 00156 Roma

SELEZIONE E AMMISSIONE

L'ammissione al corso è subordinata ad una positiva valutazione del titolo di studio richiesto per l'ammissione e del curriculum del candidato nonché ad un colloquio per verificare conoscenze informatiche, motivazione. e attitudine.

COSTO DEL CORSO

€ 2.500,00 (10% di sconto per pagamenti in un'unica soluzione) rateizzabili