Accademia Informatica s.r.l.
Viale Filippo Tommaso Marinetti 221 – 00143 Roma
Tel. 06 39746618 - Fax 06 97749271
www.accademiainformatica.com – info@accademiainformatica.com
PEC: amministrazione@pec.accademiainformatica.com
Iscrizione CCIAA di Roma n. 07153681007 - REA n. RM-1014676
Codice Fiscale e Partita IVA: 07153681007 - Cap. Soc. € 115.000,00 i.v.

CORSO DI FORMAZIONE
"Cybersecurity Technician - Gestione della Sicurezza delle Informazioni"
(QUALIFICAZIONE CYBERSECURITY TECHNICIAN - CT K1.10)
Corso di Formazione autorizzato dalla Regione Lazio con Esame di Qualificazione Professionale

DESCRIZIONE

Il Corso "Cybersecurity Technician - Gestione della Sicurezza delle Informazioni" con rilascio della Qualifica professionale di CYBERSECURITY TECHNICIAN intende preparare professionisti in grado di gestire i sistemi informativi digitali e in particolare la loro sicurezza e rispondere ai fabbisogni delle aziende di tenere traccia della sicurezza informatica relativamente agli applicativi aziendali. Il corso è rivolto a chi intenda specializzarsi nella gestione della sicurezza informatica degli applicativi aziendali e amministrare le piattaforme di proprietà, secondo le direttive di gestione e gli obiettivi imposti dalla direzione e dai *decision maker*.

Il Cybersecurity Technician è una figura professionale ampiamente richiesta dal mondo delle aziende nell'ambito dei servizi digitali, in grado di amministrare siti web e applicazioni, tenendo in considerazione la necessaria sicurezza informatica. Il Cybesecurity Technician conosce i principali *framework* e le metodologie fondamentali nell'ambito della *cybersecurity governance*. Collabora alle attività di identificazione delle fonti di rischio per la sicurezza delle informazioni e di applicazione di soluzioni idonee al ripristino del corretto funzionamento dei sistemi e delle reti. Conosce le tecnologie "disruptive" abilitanti e ne riconoscere le opportunità e i rischi ad esse correlati.

DESTINATARI

Giovani e adulti non qualificati, occupati con necessità di upskilling o reskilling, disoccupati di lunga durata con competenze informatiche di base.

REQUISITI OBBLIGATORI

- Titoli di Studio:
  - Diploma di scuola secondaria di secondo grado
- In caso di titolo di studio conseguito all'estero, è necessario presentare una dichiarazione di valore o un documento equipollente, che ne attesti la corrispondenza di valore con i titoli rilasciati nello Stato di provenienza, ai fini della verifica dei livelli di scolarizzazione.
- Per i cittadini stranieri, conoscenza della lingua italiana almeno al livello B1 del Quadro Comune Europeo di Riferimento per le Lingue, ferma restando l'obbligatorietà delle prove valutative in sede di selezione, qualora il candidato non disponga già di attestazione di valore equivalente.
- I cittadini extracomunitari devono disporre di regolare permesso di soggiorno, valido per l'intera durata del percorso.

STRUTTURA DEL CORSO

Durata ore:

- 358 ore Corso Cybersecurity Technician - Gestione della Sicurezza delle Informazioni, parte in presenza e parte in e-learning sincrono
- 150 ore Tirocinio Curriculare
- 30 ore Modulo Integrativo di Coaching & Job Placement, di cui:
  - 8 ore Orientamento Specialistico
  - 22 ore Accompagnamento al Lavoro

Durata complessiva: 538 ore / 8 mesi

Le lezioni in aula si svolgono con una frequenza di 3 gg a settimana tra il lunedì e il venerdì, e hanno durata da 4 o 6 ore.

Un numero limitato di ore di didattica potrà svolgersi in modalità Formazione a Distanza (FAD) in e-learning sincrono. Il Calendario Didattico è suscettibile di variazioni. Eventuali cambiamenti verranno comunicati agli Allievi e alla Regione Lazio.

ESAME DI QUALIFICAZIONE PROFESSIONALE
Gli allievi sono ammessi all'esame finale a condizione di avere frequentato almeno l'80% delle ore complessive del percorso formativo. Le prove finali si svolgono di fronte ad una Commissione Esaminatrice composta da un rappresentante della Regione Lazio, che la presiede; due rappresentanti dei docenti; il Responsabile Didattico; un rappresentante del Ministero dell'Istruzione e un rappresentante del Ministero del Lavoro, oltre ai rappresentanti dalle organizzazioni degli imprenditori e dei lavoratori. LIVELLO EQF DELLA QUALIFICAZIONE: 5 Codice Profilo: K1.10 - Cybersecurity Technician Diploma finale in esito ad esame ai sensi del D.lgs. 13/2013
MODALITÀ DIDATTICHE
Lezioni frontali, esercitazioni guidate individuali e di gruppo, simulazioni, analisi di casi e problem solving. Le aule sono dotate di: ▪ Postazioni docenti con leggio interattivo, computer MSI All-in-one Adora24G 2NC e sgabello; ▪ Computer per gli studenti MSI All-in-one Adora20G; ▪ LIM (Lavagna Interattiva Multimediale), munita di pennarello elettronico e collegate a videoproiettori Epson ultracorto EB 585 Wi. Modalità di valutazione degli apprendimenti Test a risposte multiple e discussione in aula al termine di ogni unità didattica, realizzazione di un Project Work e simulazione di casi.
SEDE DEI CORSI
Viale Filippo Tommaso Marinetti, 221 - 00143 Roma Tel: 06 39746618 | Fax: 06 97749271 - www.accademiainformatica.com/corsi/ E-mail: info@accademiainformatica.com
DOCENTI DEL CORSO
Andrea Dimitri, *Esperto ICT e Sicurezza Informatica, in big data analysis e machine learning, Full Stack Developer. Docente dell'Università degli Studi di Roma "Tor Vergata"* Franco Arcieri, *Ingegnere elettronico esperto in sicurezza informatica e di reti. Professore di Sistemi Cooperativi Distribuiti presso la Facoltà di Scienze dell'Università degli Studi di Roma "Tor Vergata".* Simone Ferretti, *Consulente e Formatore in Sicurezza sul Lavoro (d. lgs 81/08)* Francesca Nardelli, *Academy Manager di Accademia Informatica, Specialista di Orientamento al Lavoro* Flavia Pjetri, *Laureata in Lingue, docente di inglese* Stefano Rago, *Senior Trainer and Consultant, Ingegnere esperto di Linguaggi di programmazione* Edoardo Talamo, *Software Developer e Consulente in Sicurezza Informatica. Esperto nella progettazione e implementazione di infrastrutture software e soluzioni innovative per aziende nel settore IT.* Vincenzo Persi, *Laureato in Ingegneria delle telecomunicazioni e certificato in project management, Progettista in ambito ICT in particolare nell'ambito della sicurezza informatica. Docente nell'ambito delle discipline dell'informatica e dell'elettronica*.
SELEZIONE E AMMISSIONE
L'ammissione al Corso è subordinata ad una positiva valutazione del titolo di studio richiesto come Requisito di ammissione e del curriculum del candidato nonché al successivo superamento di un test informatico di base e un colloquio motivazionale/attitudinale. La Direzione del Corso nominerà un'apposita Commissione, incaricata di valutare preventivamente i titoli presentati dai candidati e di svolgere le prove. Al termine di ciascuna selezione i candidati riceveranno, tramite l'utilizzo dell'indirizzo di posta elettronica fornito, nota della loro ammissione o esclusione ad insindacabile giudizio della Commissione.
COSTO DEL CORSO
€ 3.900,00 10% di sconto in caso di pagamento in un'unica soluzione

Accademia Informatica s.r.l.
Viale Filippo Tommaso Marinetti 221 – 00143 Roma
Tel. 06 39746618 - Fax 06 97749271
www.accademiainformatica.com – info@accademiainformatica.com
PEC: amministrazione@pec.accademiainformatica.com
Iscrizione CCIAA di Roma n. 07153681007 - REA n. RM-1014676
Codice Fiscale e Partita IVA: 07153681007 - Cap. Soc. € 115.000,00 i.v.

PROGRAMMA DIDATTICO			
MODULO	DURATA	CONTENUTI	ARTICOLAZIONE UNITA' DIDATTICHE
MODULO 1. INTRODUTTIVO Inquadramento della professione	6 ore	Inquadramento della professione ▪ Orientamento al ruolo ▪ Elementi di diritto del lavoro, contrattualistica, regimi fiscali e responsabilità civile	Conoscenze ▪ Orientamento al ruolo ▪ Elementi di diritto del lavoro, contrattualistica, regimi fiscali e responsabilità civile
MODULO 2. INTRODUTTIVO **Elementi di base di cyber security, IT e**	66 ore	Elementi di base di cybersecurity, IT e sicurezza informatica ▪ Elementi di base di sicurezza informatica, ICT, cybersecurity ed Operational Technology	Conoscenze ▪ Elementi di base di sicurezza informatica,

sicurezza informatica		○ Introduzione alla programmazione in Python e struttura del filesystem di un pc ▪ Fondamenti di processi ed organizzazione aziendale (produzione, monitoraggio,controllo,rendicontazione) ▪ Elementi di infrastruttura IT (informatica, cloud, networking) ○ Architettura di base di un pc client e di un pc server. Dispositivi mobile. Dbms. ▪ Principali ambienti cloud (MS Azure, AWS, Google Cloud) ○ Rest web service.	ICT, cybersecurity ed Operational Technology ▪ Fondamenti di processi ed organizzazione aziendale ▪ Elementi di infrastruttura IT (informatica, cloud, networking) ▪ Principali ambienti cloud (MS Azure, AWS, Google Cloud)
MODULO 3. Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni	84 ore	Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni ▪ Principi di sicurezza informatica (RID, minimo privilegio etc…) ○ Python la libreria flask e la configurazione per l'autenticazione tls ○ I requisiti di sicurezza di un sistema informatico: autenticazione delle parti, riservatezza, integrità dei dati e dei flussi, disponibilità del servizio, robustezza e velocità dei sistemi crittografici ▪ Standard e linee guida in materia di Information Technology e Operation Technology e protezione dei dati personali ○ GDPR ovvero la legislazione europea per la protezione dei dati ▪ Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy ○ Il framework NIST per la cybersecurity e la legislazione italiana ed europea ▪ Il fattore umano nel contesto della cybersecurity ○ La figura del sistemista, dell'esperto di cybersecurity e le tecniche di social engineering ▪ Principali standard di riferimento per lo svolgimento di attività di auditing, assessment, risk assessment e risk management ▪ Metodologie di analisi delle vulnerabilità ○ Studio delle configurazioni dei sistemi sia client che server rispetto ai parametri di funzionamento e di sicurezza ▪ Best practices, standards, frameworks e principi dell'information security management ○ Configurazioni e standard di sicurezza applicate agli apparati di una infrastruttura IT ▪ Strumenti per la verifica tecnica delle vulnerabilità e degli attacchi di rete	Conoscenze ▪ Principi di sicurezza informatica (RID, minimo privilegio etc…) ▪ Standard e linee guida in materia di Information Technology e Operation Technology e protezione dei dati personali ▪ Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy ▪ Il fattore umano nel contesto della cybersecurity ▪ Principali standard di riferimento per lo svolgimento di attività di auditing, assessment, risk assessment e risk management ▪ Metodologie di analisi delle vulnerabilità ▪ Best practices, standards, frameworks e principi dell'information security management ▪ Strumenti per la verifica tecnica delle vulnerabilità e degli attacchi di rete Abilità

Accademia Informatica s.r.l.
Viale Filippo Tommaso Marinetti 221 – 00143 Roma
Tel. 06 39746618 - Fax 06 97749271
www.accademiainformatica.com – info@accademiainformatica.com
PEC: amministrazione@pec.accademiainformatica.com
Iscrizione CCIAA di Roma n. 07153681007 - REA n. RM-1014676
Codice Fiscale e Partita IVA: 07153681007 - Cap. Soc. € 115.000,00 i.v.

		○ Funzionamento delle reti locali (LAN), funzionamento delle reti server, funzionamento delle reti internet. Apparati di rete per l'instradamento e per la sicurezza (router, switch, firewall). Configurazione di pc client e server e degli apparati per l'instradamento e la sicurezza. ○ Strumenti per la verifica delle configurazioni e del corretto funzionamento di una infrastruttura IT	▪ Applicare i principi information security e cybersecurity ai processi aziendali ed alle tecnologie ▪ Supportare il team nelle attività di audit ed assessment utilizzando strumenti e metodologie idonee alla verifica degli aspetti cybersecurity ed information security ▪ Applicare attività di controllo ai sistemi informativi ▪ Svolgere attività di supporto per l'identificazione di minacce e vulnerabilità ▪ Verificare l'aderenza del sistema informativo alle normative vigenti in materia di privacy e sicurezza informatica ▪ Applicare modelli di gestione del rischio nei principali framework di riferimento ▪ Applicare modelli coerenti di analisi del rischio ▪ Effettuare attività di risk reporting e definizione dei piani di trattamento del rischio ▪ Raccogliere e analizzare le evidenze a supporto delle attività di audit, assessment ed analisi del rischio ▪ Formalizzare gli standard e le linee guida in materia di ITC ▪ Analizzare processi di business e processi di supporto, contromisure tecniche ed organizzative di natura

			cybersecurity a supporto ▪ Comprendere, comunicare ed applicare requisiti legali con impatto sulla cybersecurity ▪ Comprendere, comunicare ed applicare i requisiti di business con impatto sul governo cybersecurity ▪ Comprendere e comunicare i rischi legati al fattore umano in ambito cybersecurity ▪ Eseguire il piano di ripristino in caso di crisi
MODULO 4. Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti	84 ore	Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti ▪ Framework di riferimento in ambito IT ed OT: contromisure preventive e reattive ▪ Tassonomie, fonti in merito a minacce e vulnerabilità ▪ Principali metodologie di Vulnerability Assessment e Penetration Test o Le fasi di un Penetration test e la loro applicazione nei diversi contesti precedentemente definiti (reti, sistemi, architetture IT e OT). o La Kill Chain, le fasi di un attacco informatico e la sua applicazione nei contesti precedentemente definiti: reconnaissance, weaponization, Delivery, Exploitation, Installation, Command and control, Action on objectives/Exfiltration o La "Cyber Kill Chain Control Matrix" sua costruzione nella realizzazione degli attacchi: attacchi man in the middle, arp spoofing, session hyjacking, sql injection, attacchi al TLS e all'https, attacchi basati su tecniche di social engeenering, DOS e DDOS, buffer overflow attacks, attacchi alle reti wifi o Il protocollo ARP e la realizzazione di un ARP agent in Python ▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione degli asset informatici	Conoscenze ▪ Framework di riferimento in ambito IT ed OT: contromisure preventive e reattive ▪ Tassonomie, fonti in merito a minacce e vulnerabilità ▪ Principali metodologie di Vulnerability Assessment e Penetration Test ▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione degli asset informatici ▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione della sicurezza nell'ambito della supply chain ▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione della continuità operativa ed applicazione di modelli di disaster recovery

Accademia Informatica s.r.l.
Viale Filippo Tommaso Marinetti 221 – 00143 Roma
Tel. 06 39746618 - Fax 06 97749271
www.accademiainformatica.com – info@accademiainformatica.com
PEC: amministrazione@pec.accademiainformatica.com
Iscrizione CCIAA di Roma n. 07153681007 - REA n. RM-1014676
Codice Fiscale e Partita IVA: 07153681007 - Cap. Soc. € 115.000,00 i.v.

		▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione della sicurezza nell'ambito della supply chain
		  ○ Sicurezza nei sistemi distribuiti e attacchi realizzati su sistemi distribuiti (es. DDOS)
		▪ Framework di riferimento, pratiche, metodologie e sistemi per la gestione della continuità operativa ed applicazione di modelli di disaster recovery
		▪ Elementi di *network security*
		  ○ Libreria PYTHON scapy per l'analisi delle reti
		▪ Elementi di *web security*
		  ○ Il protocollo TLS. Le configurazioni ed i comportamenti dei browser.
		  ○ Configurazione di apache web server per il TLS. LE PKI
		▪ Elementi di *mobile security*
		▪ Modelli per la reazione e gestione degli *Incident management*
		▪ Tecniche di backup, sistemi ridondati,
		▪ Pratiche di sicurezza all'interno della tecnologia cloud
			▪ Elementi di network security
			▪ Elementi di web security
			▪ Elementi di mobile security
			▪ Modelli per la reazione e gestione degli Incident management
			▪ Pratiche di sicurezza all'interno della tecnologia cloud
			Abilità
			▪ Riconoscere ed applicare pratiche per la sicurezza dei sistemi e delle reti
			▪ Supportare il team nell'applicazione di tecniche di gestione del rischio in ambito network, web e mobile
			▪ Applicare modelli di gestione degli incidenti
			▪ Applicare modelli per la continuità operativa ed in ambito disaster recovery
			▪ Individuare e divulgare le best practices per il miglioramento delle procedure di gestione della sicurezza
			▪ Formalizzare gli standard e le linee guida in ambito cybersecurity

MODULO 5. Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie	84 ore	Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie
		
		▪ Rischi ed opportunità relativi alle tecnologie "Disruptive" abilitanti
		▪ **Principali applicazioni dell'intelligenza artificiale**
		  ○ **Anomaly detection systems e intrusion detection system costruiti usando tecniche di machine learning e intelligenza artificiale.**
		  ○ **Python applicato all'AI, progettazione di modelli di Machine Learning, costruzione di pipeline complete, utilizzo di modelli supervisionati e non supervisionati, basi dei modelli generativi.**
		▪ **Principali rischi dell'intelligenza artificiale in ambito cyber**
		▪ Modelli e rischi dell'Edge computing
		  ○ La libreria Python pandas per la gestione dei dati e le applicazioni nell'edge computing
		▪ Principali applicazioni dell'IoT e rischi correlati
			Conoscenze
			▪ Rischi ed opportunità relativi alle tecnologie "Disruptive" abilitanti
			▪ Principali applicazioni dell'intelligenza artificiale
			▪ Principali rischi dell'intelligenza artificiale in ambito cyber
			▪ Modelli e rischi dell'Edge computing
			▪ Principali applicazioni dell'IoT e rischi correlati

		○ Device di autenticazione basati su biometria, impronte digitali e riconoscimento facciale. Esempi reali di uso dell'IOT nella cybersecurity. ▪ Principali applicazioni delle tecnologie Blockchain ai diversi settori in ambito security ○ La blockchain e il ruolo dell'architettura di un sistema di servizi nella cybersecurity	▪ Principali applicazioni delle tecnologie Blockchain ai diversi settori in ambito security Abilità ▪ Comprendere e comunicare rispetto ad opportunità e rischi delle tecnologie "disruptive" abilitanti ▪ Applicare al contesto delle tecnologie "disruptive" i principi ed i principali framework di riferimento in ambito ICT, cybersecurity e protezione dei dati ▪ Comprendere e comunicare rispetto alle principali applicazioni delle tecnologie "disruptive
MODULO 6. INGLESE Inglese tecnico	26 ore	Lingua straniera tecnica ▪ Inglese tecnico per l'informatica e la cybersecurity	Conoscenze ▪ Inglese tecnico per l'informatica Abilità ▪ Comprendere, parlare, scrivere in inglese informatico
MODULO 7. SICUREZZA Operare in sicurezza nel luogo di lavoro	8 ore	Operare in sicurezza nel luogo di lavoro ▪ 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	Conoscenze ▪ Legislazione sulla salute e sicurezza sui luoghi di lavoro e applicazione delle norme di sicurezza ▪ Gli obblighi del datore di lavoro e del lavoratore
Totale corso	358 ore	Gli allievi sono ammessi all'esame finale per l'acquisizione della Qualifica Professionale di "Cybersecurity Technician" (K1.10 del Repertorio Regionale del Lazio) a condizione di avere frequentato almeno l'80% delle ore complessive del percorso formativo	
Tirocinio Curriculare	150 ore		
MODULO Integrativo Coaching & Job Placement	30 ore	▪ 8 ore Orientamento Specialistico ▪ 22 ore Accompagnamento al Lavoro	
Totale percorso	538 ore		