CORSO DI QUALIFICA PER "TECNICO DELLA SICUREZZA INFORMATICA"
AUTORIZZATO DALLA REGIONE ABRUZZO

Programma formativo

Aree disciplinari (teoriche e pratiche)	Scaletta sintetica dei contenuti e delle materie	Ore di teoria Presenza	Ore di teoria FAD
Inquadramento della professione	***Conoscenze:*** • Orientamento al ruolo; • Elementi di legislazione del lavoro e dell'impresa; • Aspetti contrattualistici, fiscali e previdenziali.	5	----
Basi di ICT	***Conoscenze:*** • Basi di ICT: architetture ed operatività dei sistemi informatici.	5	10
Fondamenti di information security e cybersecurity	***Conoscenze:*** • Principi di information security e cybersecurity; • Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy; • Standard e linee guida in materia di Information Technology, Operation Technology e protezione dei dati personali.	15	10
Supportare l'analisi di vulnerabilità, rischi e conformità	***Conoscenze:*** • Rischi relativi all'innovazione tecnologica delle ICT (intelligenza artificiale, Edge computing, applicazioni IoT, Blockchain, …); • Standard di riferimento per auditing, assessment, risk assessment e risk management applicati a sistemi digitali; • Metodi e strumenti di Vulnerability Assessment e Penetration Test; • Fondamenti di processi ed organizzazione aziendale. Potenziali impatti della vulnerabilità dei sistemi informativi sulla continuità del business.	20	10
Comunicare i rischi ed i comportamenti corretti	***Conoscenze:*** • Comportamenti umani e cybersecurity.	5	10
Supportare l'implementazione di soluzioni per la sicurezza dei sistemi hardware e software	***Conoscenze:*** • Tipologie e caratteristiche degli attacchi al sistema informativo a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente; • Caratteristiche e funzionalità dei firewall; • Caratteristiche e funzionalità dei programmi antivirus; • Caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da	40	20

	client a server; • Metodi e tecniche di configurazione del sistema di protezione e del firewall; • Modalità di autorizzazione e controllo del traffico fra reti e tipologie di tentativi di violazione delle politiche di sicurezza; • Sistemi di gestione dell'identità (IMS) ed autorizzazione degli accessi al sistema informativo ed alle reti; • Tipologie di programmi di crittografia e cifratura.		
Monitorare i sistemi hardware e software e supportare il loro ripristino in caso di problemi di integrità e sicurezza	***Conoscenze:*** • Sistemi di gestione dell'identità (IMS) ed autorizzazione degli accessi al sistema informativo ed alle reti; • Sistemi di Security Information Event Management (SIEM); • Documenti di business continuity; • Caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection; • Tecniche di disaster recovery.	30	20
Inglese tecnico per l'informatica	***Conoscenze:*** • Inglese tecnico per l'informatica.	----	10
Sicurezza sui luoghi di lavoro	***Conoscenze:*** • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza Fattori specifici di rischio professionale ed ambientale.	4	4
Totale ore presenza/FAD		**Ore presenza** 124	**Ore FAD** 94
		218	
Tirocinio		60	
TOTALE ORE CORSO		**278**	