FUTURA LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Istruzione e del Merito

Italiadomani

Regione Umbria

ITS UMBRIA ACADEMY

POST-DIPLOMA

Biennio accademico 2024_26

Corso Gratuito Durata 2 anni

Borsa di Studio fino a 6.000 €

CORSO DI STUDIO IN

CYBERSECURITY

È una figura specializzata nella protezione dei sistemi informatici e in particolare dei loro asset informativi. Il profilo acquisisce competenze trasversali digitali su IT hardware e architetture dei calcolatori, sistemi operativi e programmazione shell, reti di calcolatori e tecnologie Internet, tecniche di programmazione, basi di dati e linguaggi di interrogazione, Cloud Computing e tecnologie di virtualizzazione. Nella parte di specializzazione il profilo acquisisce competenze di Cybersecurity riguardanti vari temi e contesti, dal business, al mobile computing, con applicazioni correlate al mondo delle imprese così come per le PA. Il piano formativo differenzia il proprio ambito di intervento partendo dalla sicurezza delle reti, con contenuti relativi agli attacchi a livello di rete e di trasporto, firewall di difesa, TSL, tunneling, VPN, tecniche di machine learning per la cybersecurity. La sicurezza delle applicazioni software e dei sistemi operativi, l'amministrazione di sistema, il controllo degli accessi, la gestione e la configurazione dei servizi costituiscono parte della sicurezza di sistema. A questi si aggiungono competenze in materia di sicurezza del web, sicurezza del cloud per la gestione e la protezione degli asset di dati, sicurezza delle informazioni per l'integrità e la privacy dei dati, sia in archivio che temporanee. La figura, in termini di sicurezza di sistema viene anche formata sulle procedure di valutazione della vulnerabilità e sui test di penetrazione. Il profilo acquisisce competenze di ingegneria sociale informatica, per conoscere e prevenire le tecniche ingannevoli di condivisione dei dati personali o di apertura di link verso software malevoli. Nell'ottica delle best practice di backup e restore, sono trasferite competenze inerenti il disaster recovery, ossia le strategie con le quali si risponde a un incidente di Cybersecurity per ripristinare le operazioni, così come competenze relative l'analisi forense per individuarne le cause e il business continuity management. Il Tecnico Superiore acquisisce, inoltre, competenze di carattere organizzativo e giuridico ed è in grado di valutare la sicurezza di un sistema informatico, in ottica di Project e Risk management.

Articolazione del percorso

Il percorso formativo avrà una **durata biennale** (1.800 ore minime tra formazione – anche tramite eventuali modalità telematiche di Formazione a Distanza – e tirocinio) e **si svolgerà per più del 50% in laboratori e in azienda**, sotto la supervisione di docenti e/o tutor aziendali.
Le lezioni si svolgeranno dal lunedì al venerdì (orari tipo 9:00-13:00/14:00-18:00) indicativamente con un impegno medio d 30-35 ore settimanali.
In tirocinio si seguirà il normale orario aziendale fino ad un massimo di 40 ore settimanali
La frequenza ai corsi è obbligatoria per l'80% del monte orario.

ITS UMBRIA ACADEMY

SEDE PERUGIA

Titolo di accesso
Diploma di Scuola Secondaria di Secondo Grado o Diploma IFTS.

Titolo di studio conseguito
Diploma di Istruzione Terziaria di V livello EQF rilasciato dal Ministero dell'Istruzione.

Metodologia didattica
Docenti che provengono dalle imprese e tirocini in azienda. Metodologia didattica applicativa e laboratoriale.

Servizio di placement
Un'azione personalizzata e continuativa con elevate percentuali di assunzione

PIANO DI STUDI

	UNITA' FORMATIVA	ORE
PARTE TRASVERSALE	COMPORTAMENTO ORGANIZZATIVO	20
	INGLESE	80
	SICUREZZA	36
	INFORMATICA	140
TOTALE		**276**
PARTE SPECIALISTICA	INFORMATICA AVANZATA	70
	TECNICHE DI PROGRAMMAZIONE	30
	INTERNET TECHNOLOGIES	30
	HUMAN SECURITY	36
	SYSTEM SECURITY	252
	DATA SECURITY	70
	SOFTWARE SECURITY	72
	CONNECTION SECURITY	96
	MACHINE LEARNING	20
	ORGANIZATIONAL SECURITY	272
TOTALE		**948**
PREPARAZIONE ESAME FINALE	PROJECT WORK	10
TOTALE FORMAZIONE AULA E LABORATORIO		**1234**
TIROCINIO IN AZIENDA		**800**
TOTALE		**2034**

Competenze acquisite

- Conoscere i principi e il vocabolario della cybersecurity;
- Conoscere ed utilizzare la programmazione e lo sviluppo sicuro, il networking e le architetture di sicurezza, il web e la mobile security;
- Conoscere e saper interagire con l'organizzazione e gli strumenti di un SOC (Security Operation Center);
- Utilizzare le tecnologie per la defense e la security delle organizzazioni pubbliche e private;
- Conoscere la normativa di riferimento della sicurezza e saperla calare all'interno della Pubblica Amministrazione e dell'impresa;
- Saper utilizzare le tipologie di trust intelligence per monitoraggio e prevenzione degli attacchi cyber;
- Applicare le tecniche di risk management e saper lavorare a supporto del Data Protection Officer (DPO);
- Conoscere le tecniche per la salvaguardia dei dati in un mondo iperconnesso;
- Conoscere e saper analizzare vettori di attacco di varia natura;
- Conoscere e saper individuare le varie fasi di un test di penetrazione partendo dalla ricerca di informazioni sul target fino a sfruttare vulnerabilità;
- Conoscere e saper attuare procedure di disaster recovery, ossia delle strategie con le quali si risponde a un incidente di Cybersecurity, per ripristinare le operazioni e le informazioni, e di business continuity ossia del piano adottato;
- Conoscere e saper applicare tecniche di acquisizione forense per determinare le cause di un incidente informatico.