Soggetto proponente: Università Politecnica delle Marche, Dipartimento di Management.

Area tematica: Cyberintelligence digital investigation & social media intelligence; Intercettazioni, tecnologie, utilizzo e quadro normativo-giuridico - Reati e crimini finanziari – reati e crimini informatici - Analisi del comportamento e psicologia criminale.

Titolo del Corso: Cybersecurity, cyber risk e protezione dei dati.

Tipologia del corso: I livello.

Durata del Corso: 50 ore.

Numero massimo di iscritti: max 50

Coordinatore del corso: Prof. Antonio Di Stasi, professore ordinario presso il Dipartimento di Management, Facoltà di Economia "G. Fuà", Università Politecnica delle Marche.

Sede: Università Politecnica delle Marche, Facoltà di Economia "G. Fuà", P.le Martelli, 8 – ANCONA. La sede presenta un parcheggio interno per automobili che sarà messo a disposizione gratuitamente per frequentanti. La sede è altresì facilmente raggiungibile con i mezzi pubblici.
In caso di problemi epidemiologici da Covid-19 il Corso potrebbe essere attivato in modalità online.

Obiettivi formativi:

Il corso si pone l'obiettivo di accrescere la competenza del dipendente pubblico nell'area della cybersecurity, che coinvolge aspetti variegati ed interdisciplinari che vanno dalla protezione dei dati e delle reti alla stima del rischio cyber ed alla conoscenza delle normative vigenti in materia. In aggiunta, il corso si pone l'obiettivo di accrescere la competenza del dipendente pubblico nell'uso dei social network e sui rischi che conseguono dalla condivisione di dati su social network, sia dal punto di vista dei soggetti che li utilizzano che da quello di soggetti terzi che possano prelevare ed analizzare dati provenienti da tali infrastrutture. Infine, il corso si pone l'obiettivo di far conoscere le principali tipologie di reati informatici, con particolare riferimento all'uso delle infrastrutture tecnologiche da parte di soggetti minorenni. In sintesi, il corso ha quali obiettivi formativi lo sviluppo di nuove competenze teoriche e pratiche in termini di:

- quadro giuridico ed etico in materia di cybersecurity e protezione dei dati
- principali tecniche per la protezione dei dati e delle reti
- strumenti per la valutazione e la gestione del rischio cyber
- tecniche di social media intelligence

Indicatori di output:

Gli output saranno valutati attraverso degli indicatori analitici. Sarà valutata la capacità di conoscere i principi generali della cybersecurity e della protezione dei dati, nonché la capacità di eseguire una stima del rischio cyber e delle misure di protezione commisurate a tale rischio. Quali principali indicatori di output saranno considerati:

- La capacità di applicare tecniche di protezione dei dati nel contesto lavorativo
- La capacità di individuare e gestire elementi di rischio cyber nel trattamento dei dati
- La capacità di giudicare i rischi derivanti dalla condivisione di dati

Tali capacità verranno valutate nell'ambito di project works.

Descrizione del Corso:

Il corso è finalizzato ad accrescere le conoscenze del dipendente pubblico nell'area della cybersecurity, del rischio cyber e della protezione dei dati, con particolare riferimento ai dati personali ed alle normative che ne regolamentano la raccolta ed il trattamento.
Tali argomenti necessitano di un background tecnologico comprendente le tecniche crittografiche per la protezione dei dati e le tecniche di protezione delle reti e dei sistemi tecnologici, sulle quali si basano gli approcci progettuali per la difesa dei dati e delle infrastrutture.
Tali competenze saranno affiancate da competenze di livello gestionale, comprendenti le tecniche per la stima e la gestione del rischio cyber, necessarie anche ai fini della conformità con la vigente normativa europea sulla protezione dei dati personali.
Il corso fornirà sia competenze di natura etica e giuridica che competenze di natura tecnica, tramite il contributo congiunto di docenti provenienti dalle aree giuridiche e dell'ingegneria dell'informazione.
Il dipendente pubblico acquisirà competenze generali relative al quadro normativo e giuridico, e conoscerà le tecniche che consentono di raccogliere e trattare dati nel rispetto di tali normative e delle buone pratiche per la cybersecurity.

Sintesi del programma del Corso

- Quadro normativo sulla protezione dei dati
- Principi etici, profilazione e trasparenza
- Risk management e risk analysis
- Tecniche crittografiche per la protezione dei dati
- Autenticazione e sicurezza delle reti
- Sicurezza del software
- Vulnerability assessment e penetration testing
- Cybersecurity framework e cyber risk assessment
- Social media intelligence
- Reati informatici
- Minori e cybersecurity
- Tavola rotonda

Professori interni dell'Università Politecnica delle Marche
Prof. Antonio Di Stasi – Facoltà di Economia
Prof. Marco Baldi – Facoltà di Ingegneria
Prof. Franco Chiaraluce – Facoltà di Ingegneria
Prof. Emanuele Frontoni – Facoltà di Ingegneria
Prof. Luca Spalazzi – Facoltà di Ingegneria