POLO FORMATIVO TERRITORIALE SNA - CYBERSICUREZZA NELLA PUBBLICA AMMINISTRAZIONE: STRATEGIE, GOVERNANCE E RESILIENZA

AMBITO

Trasformazione digitale e Intelligenza Artificiale

TIPOLOGIA CORSO

CORSO SPECIALISTICO

RESPONSABILE SCIENTIFICO

NICOLA MAZZOCCA

DURATA E MODALITÀ

4gg/20h (Aula)

EDIZIONI E DATE

Vedi PAF online

OBIETTIVI AGENDA ONU 2030

['4. Istruzione di qualità', '9. Imprese, innovazione e infrastrutture']

COMPETENZE SVILUPPATE

Dirigenti
['Visione strategica', 'Gestione dei processi', 'Promozione del cambiamento', 'Decisione responsabile']

Non dirigenti
['Gestione dei processi', 'Consapevolezza digitale', 'Sostenibilità']

SEDE

Polo Formativo Territoriale SNA Calabria

OBIETTIVI E METODOLOGIA

Il corso, realizzato si propone di offrire una visione integrata e operativa delle principali tematiche legate alla sicurezza informatica della Pubblica Amministrazione, per affrontare le sfide della cybersicurezza in un contesto in continua evoluzione. Cultura organizzativa e competenze digitali sono alla base della formazione per misurarsi con le minacce digitali e gli scenari di attacco. In un quadro di gestione della sicurezza per le organizzazioni si approfondiscono alcuni degli aspetti legati alla progettazione di sistemi sicuri. La cornice normativa evidenzia i legami tra GDPR e NIS2, la nuova normativa sull'AI e il Decreto Legislativo n. 138/2024. Particolare attenzione agli aspetti di governance e al ruolo strategico dei dati: classificazione dei dati, interoperabilità, gestione del rischio e sostenibilità economica della trasformazione digitale.

Il percorso fornisce strumenti per riconoscere le principali modalità di attacco, con particolare attenzione al ruolo dell'identità digitale come punto di ingresso e controllo da un punto di vista metodologico con cenni generali agli aspetti tecnici di riferimento. Vengono approfonditi i modelli di gestione del rischio, le priorità di intervento e i principali riferimenti normativi e operativi nazionali ed europei. Il corso sviluppa inoltre consapevolezza sull'evoluzione delle minacce, inclusi gli impatti dell'intelligenza artificiale, e sul contesto strategico in cui operano le amministrazioni. Particolare attenzione è dedicata alle responsabilità dei dirigenti, alla governance della sicurezza e alla gestione degli incidenti. Le simulazioni guidate consentono di applicare le conoscenze acquisite e di esercitare capacità decisionali in contesti realistici.

PRINCIPALI TEMI

Il corso prevede di affrontare i seguenti temi:• Il contesto normativo e strategico della cybersicurezza: quadro europeo, PNRR, strategia nazionale

• Ruoli e responsabilità della PA regionale nella sicurezza informatica · Il ruolo dell'Agenzia per la Cybersicurezza Nazionale

• Competenze digitali e cultura della sicurezza nelle organizzazioni

- Minacce digitali e attacchi informatici: scenari attuali e tendenze
- Business continuity, disaster recovery e gestione del rischio
- Sicurezza Informatica, dati e intelligenza artificiale
- Progettazione e gestione in sicurezza di sistemi informativi
- Governance e modelli organizzativi per la sicurezza ICT
- Analisi di casi concreti, esperienze regionali, esercitazioni

DESTINATARI

Dirigenti e funzionari delle Amministrazioni pubbliche