

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

AMBITO

Trasformazione digitale

TIPOLOGIA CORSO

CORSO SPECIALISTICO

RESPONSABILE SCIENTIFICO

NICOLA MAZZOCCA

DURATA E MODALITÀ

 3gg/17.0h (Aula)

COMPETENZE SVILUPPATE

Dirigenti

['Decisione responsabile', 'Gestione dei processi']

Non dirigenti

['Consapevolezza digitale', 'Gestione dei processi']

OBIETTIVI E METODOLOGIA

Il corso, realizzato in collaborazione con l'Agenzia per la Cybersicurezza Nazionale, mira ad accrescere la consapevolezza strategica e organizzativa delle figure apicali regionali sui temi della cybersicurezza, rafforzando le competenze nella gestione del rischio digitale, nella definizione delle priorità e nella governance di processi di sicurezza informatica in coerenza con le strategie nazionali ed europee. La proposta formativa si profila come alta formazione a carattere tecnico-pratico, con un focus tecnico e non specialistico. Sono previsti l'analisi di casi applicativi concreti, di casi studio, simulazioni guidate. Il corso rientra nel Protocollo di collaborazione tra la Conferenza delle Regioni, la SNA e il Dipartimento della Funzione Pubblica, in attuazione del Programma di formazione 2025. In coerenza con la direttiva del Ministro per la Pubblica Amministrazione del 14 gennaio 2025 e con le priorità del PNRR, il tema della cybersicurezza è stato individuato come prioritario per il rafforzamento della capacità amministrativa e la resilienza digitale delle Regioni e delle Province Autonome.

PRINCIPALI 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