

*Webinar interattivo*

***AREA ANTICORRUZIONE, TRASPARENZA E PRIVACY***

# LA CYBER SECURITY NELLA PUBBLICA AMMINISTRAZIONE: STRATEGIE, MODELLI ORGANIZZATIVI E STRUMENTI TECNICI

**Le disposizioni della Legge 90/2024 e del D.Lgs. 138/2024 (NIS2). Le Linee guida di ACN. L'adeguamento dei modelli organizzativi. Le minacce informatiche rivolte alla PA. Le tipologie di attacchi. Il Social Engineering. Vulnerability assessment e penetration test**

## *DESCRIZIONE*

La crescente esposizione della PA agli attacchi informatici richiede un approccio integrato che combini strumenti giuridici e competenze tecniche avanzate. L'obiettivo è fornire agli operatori gli strumenti necessari per affrontare le nuove sfide della cybersicurezza, in linea con il quadro normativo nazionale ed europeo.

Il webinar offre un inquadramento completo in materia di cyber security per il settore pubblico, integrando competenze giuridiche e tecniche. Viene approfondito il ruolo di ACN, le novità introdotte dalla L. 90/2024 e dal D.Lgs. 138/2024 (NIS2), con particolare attenzione ai modelli organizzativi e ai profili di responsabilità delle figure coinvolte. Sotto il profilo tecnico sono affrontate le principali minacce informatiche per la PA, gli strumenti di difesa e le attività di prevenzione, come i vulnerability assessment e i penetration test.

## *PROGRAMMA*

- **La cyber security nel settore pubblico**: lo stato dell'arte e gli scenari futuri.
- **Il ruolo dell'Agenzia per la Cybersicurezza Nazionale** (ACN).
- **Le disposizioni della Legge 90/2024**: rafforzamento della cybersicurezza nazionale e reati informatici. Le **Linee guida di ACN**.
- **Il D.Lgs. 138/2024 di recepimento della direttiva (UE) 2022/2555**: le misure per un livello comune elevato di cybersicurezza nell'UE. Il **NIS - Network Information Security**.
- **L'adozione di un Modello organizzativo di gestione della cyber security** (D.Lgs. 138/2024). La revisione dei regolamenti interni e delle policy.
- **La nomina di un Responsabile per la sicurezza informatica con competenze specifiche in materia di cybersicurezza** (D.Lgs. 138/2024). Gli obblighi formativi.
- I **profili di responsabilità** delle diverse figure coinvolte.
- **La sicurezza informatica dal punto di vista tecnico**. I concetti di base: **Cybersicurezza e Cyberspazio**.
- **La protezione delle informazioni**: sicurezza fisica e logica; protezione dei dati personali; anonimizzazione.
- **Gli attacchi**: tipologie, finalità e principali cause che ne favoriscono la riuscita.
- **Il Social Engineering**: tassonomia dei vettori di attacco più comuni nell'ambito dell'ingegneria sociale.
- **Gli strumenti di difesa**: gestione delle credenziali; crittografia; segmentazione e sicurezza della rete.
- **La attività di prevenzione**: vulnerability assessment, penetration test, simulazioni di attacchi controllati, mappatura delle superfici di attacco.

PROMOPA FONDAZIONE
RICERCA ALTA FORMAZIONE PROGETTI

**Michele Morriello**
Avvocato, Esperto di PA digitale e privacy
**Rocco De Nicola**
Ordinario di Informatica, già Rettore della Scuola IMT Alti Studi

**3 dicembre 2026**
Orario 9.30-13.30

**Euro 280,00 + IVA se dovuta**
La quota di partecipazione è comprensiva di **materiale didattico** e **registrazione video** del webinar

**Riduzione del 15%** in caso di iscrizione di più persone: quota di partecipazione individuale Euro 235,00 + IVA se dovuta

**Attestato di partecipazione con profitto**, idoneo ai fini dell'obbligo formativo di cui alla Direttiva Zangrillo del 14/1/2025.