

UCBM ACADEMY

EXECUTIVE PROGRAM

CYBERSECURITY E RESPONSABILITÀ DEI VERTICI SANITARI AI SENSI DELLA DIRETTIVA NIS2

Rischio legale, dati clinici e continuità operativa

Quando la cybersecurity diventa responsabilità strategica

Nel settore sanitario, la cybersecurity non è più soltanto una questione tecnologica, ma un tema di governance, continuità operativa e tutela del paziente. Le organizzazioni sanitarie gestiscono dati clinici sensibili, infrastrutture critiche e processi essenziali che, se compromessi, possono generare conseguenze rilevanti sul piano giuridico, organizzativo e reputazionale.

Con il recepimento della Direttiva (UE) 2022/2555 – NIS2 attraverso il D.Lgs. 138/2024, i vertici delle organizzazioni sono chiamati ad assumere un ruolo diretto nella supervisione del rischio cyber, con obblighi non delegabili, responsabilità personali e un nuovo regime sanzionatorio.

Perché l'Executive Program Cybersecurity e Responsabilità dei Vertici Sanitari ai sensi della Direttiva NIS2?

In uno scenario in cui le minacce cyber sono sempre più frequenti e sofisticate, il vero fattore distintivo non è soltanto l'adozione di misure tecniche, ma la capacità del management di:

- comprendere il perimetro delle proprie responsabilità;
- presidiare il rischio sanzionatorio;
- assumere decisioni corrette, documentate e tracciabili;
- coordinare in modo efficace la gestione degli incidenti;
- integrare la cybersecurity nei processi di governance.

L'Executive Program nasce per offrire a figure apicali e dirigenti strumenti concreti per affrontare la cybersecurity come leva di responsabilità strategica e organizzativa.

Cosa imparerai?

Al termine dell'Executive Program, sarai in grado di:

- interpretare correttamente gli obblighi previsti dalla Direttiva NIS2;
- comprendere il perimetro delle responsabilità dei vertici nelle organizzazioni sanitarie;
- individuare e ridurre il rischio sanzionatorio;
- assumere decisioni informate, corrette e conformi alla normativa;
- supervisionare la gestione degli incidenti cyber;
- contribuire alla definizione di una strategia di cybersecurity efficace.

Destinatari e requisiti di accesso

Il corso si rivolge a figure apicali e dirigenziali, con particolare riferimento al settore sanitario, e in particolare a:

- Direzione generale, sanitaria e amministrativa;
- responsabili di funzione e coordinatori di area;
- professionisti coinvolti nella gestione del rischio e della compliance;
- manager operanti in contesti sanitari pubblici e privati;
- figure chiamate a presidiare processi decisionali con impatti su sicurezza, continuità operativa e gestione dei dati.

Direzione Scientifica

Prof. Roberto Setola

Professore Ordinario di Automatica e Direttore Scientifico del Master in Homeland Security
Università Campus Bio-Medico di Roma

Faculty

La faculty è composta da esperti in cybersecurity, diritto delle tecnologie e governance sanitaria, con esperienza diretta in contesti complessi e regolati.

Struttura dell'Executive Program

L'Executive Program si articola in **2 giornate consecutive**. Le attività si svolgeranno **in presenza presso UCBM Academy, Via Amsterdam 125 – 00144 Roma**, con la possibilità di partecipare anche da remoto, previa comunicazione.

Giornata	Orario	Modulo	Argomenti
Giovedì 12 novembre 2026	15:00 – 18:00	**Scenario, NIS2 e responsabilità dei vertici**	Trasformazione digitale e rischi cyber; scenario della cybersecurity nel settore sanitario; valore strategico e criticità dei dati sanitari. Inquadramento NIS2 e responsabilità apicali (D.Lgs. 138/2024); obblighi non delegabili; ruolo dei vertici. Implementazione delle misure minime ACN: policy, procedure e presidi di sicurezza; governance della cybersecurity. Regime sanzionatorio e profili di responsabilità; impatti reputazionali e istituzionali.
Venerdì 13 novembre 2026	09:30 – 12:30	**Governance e responsabilità**	Risk management e fattore umano; principi di cyber risk management; cultura della sicurezza. Responsabilità per decisione e mancata decisione; tracciabilità e supervisione.
	13:30 – 17:00	**Gestione del rischio e crisi**	Riduzione del rischio sanzionatorio; analisi del livello di maturità e azioni chiave. Incidenti cyber e conseguenze sanzionatorie; obblighi di notifica e ruolo dei vertici. Gestione delle emergenze cyber; simulazioni (ransomware, data breach) e decision-making nelle fasi critiche. Ultimi 30 minuti dedicati al test finale di verifica dell'apprendimento.
	17:00 – 17:30		**Test Finale e consegna attestati**

Quote di partecipazione

Quota di partecipazione: € 1.200,00.

Sono previste agevolazioni e possibilità di finanziamento tramite fondi interprofessionali (Fondimpresa, Forte, Fondirigenti, ecc.).

Attestati e certificazioni

Al termine del corso, i partecipanti riceveranno un attestato di partecipazione rilasciato dall'Università Campus Bio-Medico di Roma, rilasciato ai sensi dell'art. 23, comma 2, lett. a) del D.Lgs. 4 settembre 2024, n. 138.

Modalità di Iscrizione

Per iscriversi, è sufficiente compilare il form online disponibile nella pagina dedicata, accessibile cliccando qui
o inquadrando il QR-code.



Il valore distintivo di UCBM Academy nella Sicurezza Integrata

UCBM Academy si distingue nella formazione in ambito Sicurezza Integrata per un approccio sistemico e multidisciplinare che supera le tradizionali distinzioni tra sicurezza fisica, cybersecurity, intelligence, geopolitica e protezione delle infrastrutture critiche.

La sicurezza è oggi un dominio profondamente interconnesso, in cui Homeland Security, Cybersecurity, Space Security, gestione del rischio, governance delle informazioni e resilienza organizzativa rappresentano dimensioni complementari di un unico ecosistema. UCBM Academy affronta tali ambiti come elementi di un quadro strategico unitario e integrato.

Attraverso l'integrazione tra ricerca scientifica, competenze tecnologiche e visione strategica – e grazie alla collaborazione con istituzioni e aziende operanti nei settori della sicurezza nazionale e internazionale - l'Academy trasferisce nei propri percorsi formativi una prospettiva concreta, fondata su casi reali, analisi di scenari evolutivi e applicazioni operative.

Formarsi in questo contesto significa sviluppare una visione integrata della sicurezza come fattore critico di competitività, stabilità e innovazione, acquisendo strumenti analitici e decisionali per governare contesti complessi e ad alta incertezza.

In Partnership con:

mead
YOUR DIGITAL INTEGRATOR



UCBM ACADEMY

Università Campus Bio-Medico di Roma
Email: ucbmacademy@unicampus.it
Telefono: 06.22541.9300
https://ucbmacademy.unicampus.it/