In convenzione con

CORSO DI FORMAZIONE AVANZATA

CYBER LAW AND SECURITY

nell'era dell'AI oltre la cybersecurity

Premessa e contesto strategico

Negli ultimi anni, la trasformazione digitale ha profondamente modificato il concetto stesso di sicurezza, imponendo un ripensamento radicale delle tradizionali categorie giuridiche ed economiche. Le organizzazioni pubbliche e private non operano più come entità isolate, ma come nodi di ecosistemi complessi, interconnessi e fortemente interdipendenti. In questo contesto, la cybersecurity non rappresenta più una funzione tecnica circoscritta all'ambito IT, bensì un elemento strutturale della stabilità economica, della continuità dei servizi essenziali e della sicurezza nazionale.

L'evoluzione del quadro normativo europeo, con l'introduzione di strumenti quali la Direttiva NIS2, il Regolamento DORA e l'AI Act, evidenzia come la sicurezza informatica sia oggi considerata una componente fondamentale della governance pubblica e privata. Parallelamente, a livello nazionale, il Perimetro di Sicurezza Cibernetica ha rafforzato ulteriormente l'approccio sistemico alla protezione delle infrastrutture strategiche.

Allo stesso tempo, la natura delle minacce si è evoluta in modo significativo. Gli attacchi informatici non si limitano più alla compromissione di sistemi tecnologici, ma si inseriscono in strategie più ampie di guerra ibrida, che includono disinformazione, pressione economica e destabilizzazione istituzionale. In tale scenario, la cybersecurity assume una dimensione giuridica, economica e geopolitica, richiedendo nuove competenze interdisciplinari.

Finalità del Corso

Il Corso di Alta Specializzazione in "Cybersecurity e Difesa delle Infrastrutture Strategiche nell'Era dell'AI e della Guerra Ibrida" si propone di formare figure professionali in grado di comprendere e governare la sicurezza informatica come fenomeno complesso, multidimensionale e strategico.

L'obiettivo principale è superare l'approccio meramente tecnico alla cybersecurity, integrando prospettive giuridiche, economiche e organizzative, al fine di sviluppare competenze avanzate nella gestione del rischio, nella compliance normativa e nei processi decisionali.

Il corso mira inoltre a fornire strumenti operativi per l'analisi delle responsabilità, la valutazione degli impatti economici degli incidenti cyber e la gestione delle crisi, con particolare riferimento alle infrastrutture strategiche e ai servizi essenziali.

Destinatari

Il Corso è rivolto a laureati in discipline **giuridiche, economiche, politiche e STEM**, dirigenti e funzionari della Pubblica Amministrazione, Forze dell'Ordine, manager e responsabili aziendali, consulenti, avvocati e professionisti della **CYBERSECURITY** e della compliance

Il percorso è inoltre particolarmente indicato per figure coinvolte nei processi decisionali e nella gestione del rischio, anche in contesti complessi e ad alta criticità.

Struttura Didattica

Il corso è così strutturato:

100 ORE DI LEZIONI FRONTALI IN FAD

100 ORE DI STUDIO INDIVIDUALE

30 ORE DEDICATE ALL'ELABORAZIONE TESI

La struttura segue una progressione logica che parte dall'analisi del contesto geopolitico e normativo, per poi approfondire i temi della regolazione europea e nazionale, della governance e della compliance, fino ad arrivare agli aspetti economici, alla gestione degli incidenti e alla digital forensics.

Particolare rilievo è attribuito al collegamento tra normativa e applicazione pratica, con un'attenzione costante alle implicazioni operative per imprese e pubbliche amministrazioni.

Modulo 1 – Geopolitica della Cybersecurity e Guerra Ibrida

Modulo 2 – Fondamenti di Cybersecurity per Giuristi ed Economisti

Modulo 3 – International Cybersecurity Law

Modulo 4 – Diritto Europeo della Cybersecurity

Modulo 5 – NIS2 e Compliance delle Infrastrutture Strategiche

Modulo 6 – Perimetro Nazionale di Sicurezza Cibernetica

Modulo 7 – Diritto Pubblico dell'Intelligenza Artificiale

Modulo 8 – Economia della Cybersecurity e Risk Management

Modulo 9 – Governance, Compliance e Responsabilità d'Impresa

Modulo 10 – Digital Forensics per le Imprese

Modulo 11 – Incidenti Cyber e Responsabilità Legale

Modulo 12 – Inglese Tecnico

Modulo 13 – Laboratorio Finale e Casi Studio

Docenti

- Dott. Adriano Avenia, Fondazione Ugo Bordoni, Esperto in Cybersecurity, Cloud, Sovranità Digitale e Sicurezza delle Infrastrutture Critiche
- Prof. Avv. Filippo Bianchini, UNIPG, Avvocato Cassazionista Esperto di Protezione Dati Personali, Cybersecurity e Intelligenza Artificiale
- Dott. Domenico Campeglia, Formed Aps e Consulente Didattico, Cyber Security Specialist & Dfir Analyst Vatican Cyber Volunteers
- Dott. Cataldo Dammacco, UNIBA, Esperto di Diritto, Organizzazione e Gestione della Sicurezza Informatica
- Prof. Paolo Dal Checco, UNITO, Consulente Informatico Forense, Esperto di Sicurezza Informatica
- Avv. Annamaria Di Legge, UNICAS, Docente in "Data Protection and Scientific Research: GDPR Codes Of Conduct" e "International Cyber Law"
- Ing. Carmelo Di Mauro, National Cyber Competence Center (NC3) del Lussemburgo, Esperto In Analisi e Gestione del Rischio
- Dott.ssa Mariateresa Fappiano, UNICAS, Dottore di Ricerca in Diritto Internazionale e Professore a Contratto
- Prof. Avv. Francesco Maiello, UNICAS, Docente di Diritto Internazionale Privato, Esperto in Cybersecurity
- Prof. Avv. Francesco Mazza, UNICAS, Docente di Diritto Penale, Esperto in Cybersecurity e Diritto Penale Dell'informatica
- Avv. Nicola Montesano Cancellara, UNICAS, Dottorando di Ricerca in Diritto Internazionale dello Spazio
- Prof. Avv. Francesco Paolo Micozzi, UNIPG, Esperto in Informatica Giuridica e Cybersecurity
- Prof. Ing. Ugo Lopez, UNIBA, Professor of Ethics, Privacy & Security
- Prof. Avv. Tommaso Alessio Salemme, UNICAS, Professore di Cyber International Law e di Contrattualistica Internazionale
- Prof. Avv. Giancarlo Scalese, UNICAS, Ordinario di Diritto Internazionale, Presidente dei Servizi Giuridici per Lavoro, Pubblica Amministrazione, Sport e Terzo Settore
- Prof.ssa Avv. Annita Larissa Sciacovelli, UNIBA, Coordinatrice della "Winter Cyber School", Docente del Cyber Lab di Diritto Internazionale ed Europeo della Cybersicurezza