CE/DA Centro Italiano di Direzione Aziendale Srl
00185 Roma - Via Palestro, 24 – Tel 06.49.25.31

Y1
Cybersecurity nelle organizzazioni negli scenari dell'intelligenza artificiale

DURATA
3 giorni

DATA
3-10-11 giugno 2025

ORARIO
9,00 – 14,00

QUOTA DI PARTECIPAZIONE
euro 800,00 + IVA (la quota è esente da IVA se corrisposta da Enti pubblici)

RELATORE
Avv. Mauro ALOVISIO
Avvocato presso l'Università di Torino, si occupa di diritto delle nuove tecnologie, docente presso il master cybersecurity dell'Università degli Studi di Torino, coordinatore del corso di perfezionamento in materia di protezione dei dati personali dell'Università di Torino formatore e autore di pubblicazioni e articoli in materia di cybersecurity, Nis 2, GDPR e intelligenza artificiale, direttore del Centro Studi di Informatica Giuridica di Ivrea Torino
Dott. Marco CRIMI
laureato in Scienze Politiche e Scienze Strategiche, Cybersecurity e Blockchain Specialist, NFT certified, VR&AR professional. Founder di Vivon 4.0, start-up innovativa che utilizza tecnologia blockchain propria per tracciare la filiera nell'agrifood, eliminando l'intervento umano e assicurando l'integrità dei dati attraverso IoT e IA. Advisor per numerose organizzazioni, il background e l'esperienza gli permettono di condividere un'ampia conoscenza operativa in tema di protezione dei dati e infrastrutture digitali, con un focus su tecnologie emergenti e sicurezza delle reti decentralizzate.

INTRODUZIONE
La cybersecurity è strategica per la competitività del nostro paese e per l'erogazione di servizi ai cittadini e per i diritti e le libertà delle persone ed è al centro dell'agenda europea e nazionale con numerose novità normative con impatto sul settore pubblico e privato. L'Italia è la nazione in Europa con il maggior numero di attacchi informatici.

OBIETTIVI
Gli attacchi informatici sono aumentati sia in termini quantitativi e qualitativi e hanno ad oggetto anche infrastrutture, servizi web e siti della pubblica amministrazione con gravi danni alle imprese, al nostro sistema economico e alla reputazione e credibilità del nostro paese.

Il percorso formativo è finalizzato a sensibilizzare il personale sui rischi, sulle misure organizzative e tecniche per prevenire e contrastare gli incidenti di sicurezza e le violazioni dei dati e a illustrare le ultime novità normative, le sanzioni e le responsabilità in materia

I formatori sono esperti in materia, docenti in master universitari e presso associazioni datoriali e sono autori di molteplici pubblicazioni.

DESTINATARI
responsabili ICT, CISO, referente cybersecurity, responsabili della transizione digitale, amministratori di sistema, responsabili del personale di enti e società pubbliche e private, avvocati, consulenti e DPO

CONTENUTI

Il corso illustra le principali novità normative e i relativi impatti sulle organizzazioni, sulle persone e sulle responsabilità con un taglio interdisciplinare e presentazione di casi concreti finalizzati a trasferire la consapevolezza del tema, le informazioni utili e la conoscenza degli strumenti in materia da utilizzare nelle attività quotidiane

METODOLOGIA

Il corso ha un taglio operativo e articolato in cinque sessioni e prevede, in ottica accountability, a tutela dell'amministrazione anche esercitazioni e un quiz finale di verifica dell'apprendimento con scenari e dinamiche di gaming

MATERIALE DIDATTICO

Specificare il tipo di materiale didattico fornito che sarà poi disponibile su Moodle

PROGRAMMA

Per ciascuna sessione specificare i punti trattati

SESSIONE 1 – 3 giugno 2025

- Presentazione del corso, dei docenti e degli allievi
- Gli attacchi informatici: dati ed evoluzioni, gli attacchi più comuni ad un'organizzazione: ganoramica generale Statistiche Chiave - Aumento degli Attacchi, Settori Maggiormente Colpiti
- La definizione ed evoluzione della sicurezza informatica e della cibersecurity: perché ci riguarda tutti? esempi concreti e best practice
- Gli attacchi ransomware, Il danno reputazionale e i nuovi scenari di danno erariale
- Cybersecurity e GDPR
- Il ruolo della form- azione: quali obblighi? Quali errori non commettere?
- Il fattore umano e i ruoli nelle organizzazioni alla luce della Nis 2 e della legge 90 del 2024; le figure (Responsabile Transizione digitale, Referente per la cibersicurezza, il punto di contatto, il responsabile del personale, il responsabile della prevenzione della corruzione e della trasparenza, il responsabile della conservazione dei documenti, il responsabile degli approvigionamenti)
- La visione europea: Il cybersecurity Act ed il ruolo dell'Enisa e i nuovi scenari del cybersecurity Resilience Act
- Il perimetro cibernetico nazionale (soggetti, notifiche, misure di sicurezza, sanzioni e responsabilità)
- Le direttive Network and Information Systems (NIS 1 e 2)
- Il ruolo dell'Agenzia per la cybersicurezza nazionale (ACN) e dello Csirt
- Il Piano Triennale per l'informatica: misure richieste, scadenze e responsabilità, profili regolatori e impatti
- La nuova legge 90 in materia di cybersecurity nel settore pubblico: l'ambito di applicazione, impatto e la road map
- Il nuovo referente cybersecurity; compiti, responsabilità e impatto organizzativo, il monitoraggio delle vulnerabilità e lo strumento della crittografia, impatto sui reati e sui modelli 231
- L'ambito di applicazione della Nis 2 e la road map Impatto sulla governance; le novità sulla formazione; responsabilità e sanzioni, l'iscrizione alla piattaforma di Acn e gli obblighi di notifica. Quiz finale di apprendimento

SESSIONE 2 – 10 giugno 2025

- La gestione degli attacchi e l'analisi del rischio

- Tipologie di attacchi (Malware, Phishing, Data Breatches, Attacchi DDoS,BEC/Man in the Middle, Sim Swap Il modello «Crime as a service» ed esempi di crimine su darkweb: Ransomware-as-a-service)
- Impatto Economico e Fattori di Rischio
- Evoluzione delle Tecniche di Attacco
- L'importanza della consapevolezza sugli attacchi informatici
- Framework Nazionale per la Cybersecurity e Data Protection
- La notifica degli incidenti allo Csirt , le novità e gli impatti
- Esercitazione collettiva di notifica al Garante e allo Csirt
- Business Impact Analysis (BIA)
- Metodologie ENISA
- Metodologie NIST 1 e 2: punti di forza e impatto per gli enti
- Gli strumenti delle ISO 27001 e la ISO62443
- Strumento della Relazione Tecnica e degli Audit Informatici
- Analisi della vulnerabilità alle tecniche di ingegneria sociale

SESSIONE 3 – 11 giugno 2025

- Le misure organizzative e i nuovi scenari della cybersecurity
- Security by design: l'approvvigionamento di software e app alla luce della legge 90 del 20924
- La supply chain : le misure di sicurezza e le best practice su audit filiera dei fornitori
- GDPR: le ispezioni del Garante e le sanzioni in ambito Cybersecurity ,Simulazione di ispezione del Garante privacy
- Sanzioni amministrative e i nuovi scenari di danno erariale connesse alla mancata adozione delle misure di sicurezza nell'ambito pubblico
- Le policy sulla scelta e aggiornamento delle password e su utilizzo di posta elettronica ed internet
- Le novità dei Reati informatici: caso concreto: l'accesso abusivo del dipendente infedele, l'evoluzione della giurisprudenza Responsabilità 231: modelli organizzativi, quali errori non commettere, Cenni sulla digital forensics
- I nuovi scenari cybersecurity, Internet degli Oggetti e Intelligenza artificiale: deep fake. Gli strumenti a tutela
- Policy: come utilizzare l'intelligenza artificiale negli enti pubblici: le linee guida Agid
- Il deep fake nel regolamento europeo e nella normativa nazionale; strumenti di prevenzione e contrasto
- Lo strumento delle assicurazioni cyber
- Lo strumento della blockchain
- Conclusioni del corso

RILASCIO ATTESTATO DI FREQUENZA E PROFITTO

Il CEIDA**, Ente accreditato dalla Regione Lazio** quale soggetto erogatore di attività per la Formazione Superiore e Continua, (accreditamento ottenuto con Determinazione del Direttore della Dir. Reg. "Formazione, Ricerca e Innovazione, Scuola e Università, diritto allo studio" n. G16019 del 23/12/2016, pubblicata sul B.U.R.L. n. 2 del 5/1/17), attesta, per ogni partecipante, le caratteristiche del percorso formativo e quanto di questo è stato effettivamente frequentato, attraverso rilascio degli attestati di frequenza subordinatamente al superamento di una verifica finale attuata mediante questionario a risposta multipla.