Master Specialistico

MASTER in CYBERSECURITY MANAGEMENT

Governance e strategia della cybersecurity, risk assessment, sicurezza delle informazioni, conformità NIS2 e DORA, business continuity e gestione degli incidenti: il Master operativo per chi gestisce i rischi cyber in azienda

In Live Streaming dal 02/04/2027

LIVE STREAMING - Programma Dettagliato delle Lezioni

CYBERSECURITY & COMPLIANCE SECURITY MANAGEMENT

Sicurezza informatica, Sicurezza delle informazioni, Governance e visione strategica della cybersecurity, processi di conformità, analisi dei rischi e delle minacce, business continuity, perimetro nazionale di sicurezza cibernetica

Lezione 1 , Venerdì 02/04/2027 (pomeriggio)

Fondamenti di Cybersecurity: Information Security Governance

- Missione dell'information security: Triade CIA
- Information Security Governance
  - Ruoli, Responsabilità metriche di Governance
  - Information Security Strategy
- Overview – Information Risk e Compliance
  - Determinare lo stato di maturità dell'Information security
  - Sviluppo di una strategia
- Sviluppo di un programma di information security
  - Obiettivi di programma e scelta di un framework
  - Definizione di una roadmap e implementazione
- Gestione di incidenti di information security
  - Risorse, obiettivi e indicatori
  - Business Continuity e Disaster Recovery
- Esercitazione:
  - Verifica di un programma di Information Security

Lezione 2 , Sabato 03/04/2027 (mattina)

Cybersecurity Risk Assessment: Nozioni tecniche di base e Open-sources threat analysis

- Nozioni base di architettura dei sistemi
- Threats
  - Internal and External
  - Advanced Persistent Threat and Emerging Threats
  - MITRE att&ck, SANS
- Vulnerabilities
  - National Vulnerability Database
  - OWASP Top 10:2025 – principali rischi applicativi aggiornati (incluse le nuove categorie: Software and Data Integrity Failures, Supply Chain Security)

Esercitazione:

- Password cracking

Lezione 3 , Venerdì 09/04/2027 (pomeriggio)

Laboratorio di cyber security: Malicious cybersecurity activities e tecniche di business continuity

- Situazione degli attacchi riusciti nel mondo e in Italia suddivisi per tipologia d'attacco, vittime, luoghi e tecniche – con dati aggiornati all'edizione più recente del Rapporto Clusit
  - Esempi di attacchi riusciti
- Principali tecniche d'attacco

        - DOS e DDOS
        - Data exfiltration
        - Phishing
        - Defacement
        - Malware e Ransomware: evoluzione recente delle campagne e tecniche di delivery
        - Supply chain attack: attacchi attraverso la filiera software e dei fornitori
    - Tecniche di difesa
        - Business continuity
        - Disaster Recovery
        - patch management

Lezione 4 , Sabato 10/04/2027 (mattina)

Risk Assessment Cybersecurity: analisi e contestualizzazione delle minacce

- Analisi e trattamento del rischio cyber
- Episodi eclatanti di incidenti di sicurezza
- Evoluzione delle minacce e degli attori
- ENISA Threat Landscape,
- Panoramica delle principali minacce
- MITRE ATT&CK
- Metodologie di analisi del rischio: OCTAVE, ISO 31000, framework NIST
- Case study Risk Analysis

Lezione 5 , Venerdì 16/04/2027 (pomeriggio)

Laboratorio di cyber security: Nozioni tecniche avanzate

- Sicurezza dei dati
- Cloud security: vantaggi, rischi e modelli di responsabilità condivisa (Shared Responsibility Model)
- Crittografia (cosa è e a cosa serve)
- Steganografia (cosa è e a cosa serve)
- Breve storia della crittografia
- Crittografia classica
    - simmetrica
    - asimmetrica
    - firma elettronica
- Cenni di crittografia avanzata
- Introduzione ai rischi di sicurezza legati all'Intelligenza Artificiale (AI): AI come vettore di attacco e come strumento di difesa; cenni sulle principali vulnerabilità dei sistemi basati su AI generativa (es. prompt injection, data poisoning)

Lezione 6 , Sabato 17/04/2027 (mattina)

Normative e Best practices di riferimento della cybersecurity

- Normative Cybersecurity UE ed ITA
- Perimetro Strategico Nazionale Cybersecurity
- Standards & Best Practices Cybersecurity
- Sistemi di gestione
- ISO/IEC 27001:2022 e 27002:2022 – struttura aggiornata (93 controlli, 4 domini; nuovi controlli su threat intelligence, cloud, data masking, secure coding)
- ISO 22301 - Business Continuity
- Case study BIA
- Case Study DRP
- Standard USA: NIST CSF 2.0 (con la nuova funzione Govern), CIS Controls v8, NIST SP 800-53 rev.5
- Case study NIS2 & DORA: entrambe le normative sono ora pienamente operative – analisi degli impatti organizzativi e delle misure di conformità richieste alle aziende

Lezione 7 , Venerdì 07/05/2027 (pomeriggio)

L’importanza della sicurezza fisica nella sicurezza informatica

- Fondamenti di Sicurezza Fisica e Security Convergence

- Analisi di dettaglio controlli di sicurezza fisica ISO/IEC 27001:2022 (Annex A, dominio Physical Controls)
- I controlli di sicurezza fisica nello Standard NIST SP800-53
- Sicurezza e sorveglianza nei Data Center
- Trasferimento delle responsabilità
- Cloud & Shared Reponsibility Model
- Case Study: Supernap & Google

Lezione 8 , Sabato 08/05/2027 (mattina)

Cybersecurity risk management: Cybersecurity plan e Cybersecurity Management

- Progettazione e sviluppo di un Cybersecurity plan
  - Elementi essenziali
  - SWOT analysis e ROI del cybersecurity plan
- Processi del Sistema di gestione dell'Information security
  - Risk management
  - Incident and Change management
  - Internal audit, valutazione delle performance e processo di miglioramento
- Gestione della sicurezza nella supply chain: rischi derivanti da fornitori e partner tecnologici; principi di vendor risk management

Lezione 9 , Venerdì 14/05/2027 (pomeriggio)

Competenze e consapevolezza in materia di cybersecurity

- Concetti fondamentali
- Le competenze secondo la ISO/IEC 27021
- European Cybersecurity Skills Framework
- Panoramica formazione e certificazioni personali
- Programmi di formazione del cittadino ed aziendali
- Case study: "Secure The Humans!" tramite programma aziendale SAT
- AR-in-a-Box

Lezione 10 , Sabato 15/05/2027 (mattina)

Fondamenti di Cybersecurity: Fondamenti Normativi

- NIS 1: evoluzione storica e superamento (Direttiva UE 2016/1148, recepita con D.Lgs. 65/2018 – ora abrogato)
- NIS 2 e il suo recepimento in Italia: quadro degli obblighi, soggetti interessati (essenziali e importanti), ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) come autorità competente; principali scadenze operative
- EU-Cybersecurity Strategy
- EU-Cybersecurity Act (Reg. UE 2019/881) e il ruolo di:
  - European Network and Information Security Agency (ENISA);
  - CERT-EU / ENISA CERT
  - Computer Security Incident Response Team (CSIRT);
- European Cyber Security Organisation (ECSO).
- Perimetro Cibernetico Nazionale
  - Decreto Legge 21 settembre 2019, n. 105
  - DPCM 131/2020 del 21 ottobre 2020
- Decreto legislativo 8 giugno 2001, n. 231 e i reati informatici
- Cyber Resilience Act (Reg. UE 2024/2847): obblighi di sicurezza per prodotti con elementi digitali; principali adempimenti applicabili dal 2026
- DORA (Reg. UE 2022/2554): resilienza operativa digitale nel settore finanziario – quadro degli obblighi e stato di applicazione

Lezione 11 , Venerdì 21/05/2027 (pomeriggio)

Il contributo della Funzione Compliance nel processo di ICT Compliance

- Governo e organizzazione del sistema presidio della sicurezza informatica
  - Ruolo degli Organi Aziendali
  - Ruolo delle Funzioni Aziendali di Controllo
  - Ruolo della Funzione ICT e della Funzione di Sicurezza Informatica

        - Caso Partico: Organizzazione Cybersecurity di Avio SpA
        - Esercitazione "Attacco Ransomware": gestione della crisi, intervento degli Organi Aziendali e profili di responsabilità ex D.Lgs. 231/2001
        - Presidio delle Esternalizzazioni ICT
    - Il contributo della Compliance per le tematiche di Compliance ICT
    - Perimetro normativo di ICT Compliance: quadro aggiornato NIS2, DORA, Cyber Resilience Act e riflessi sulla funzione Compliance

Per esigenze di natura organizzativa e didattica, la Scuola si riserva la facoltà di rinviare, di modificare, così come di spostare le date delle lezioni rispetto al calendario inizialmente prestabilito. Inoltre, si riserva il diritto di modificare in ogni momento i contenuti, dei programmi ed il corpo docente al fine di perseguire miglioramenti didattici in linea con i cambiamenti di mercato e le subentrate esigenze organizzative.