

## 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

Webinar dal 9 giugno all'8 luglio 2022

### Lezione I - Giovedì 09/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)

#### Fondamenti di Cybersecurity: Fondamenti Normativi

- Perimetro Cibernetico Nazionale
  - Decreto Legge 21 settembre 2019, n. 105
  - DPCM 131/2020 del 21 ottobre 2020
- EU-Cybersecurity Strategy
- EU-Cybersecurity Act – Regulation (EU) 2019/881 e il ruolo di:
  - European Network and Information Security Agency (ENISA);
  - Computer Emergency Response Team (CERT-EU);
  - Computer Security Incident Response Team (CSIRT);
  - European Cyber Security Organisation (ECSO).
- Decreto legislativo 8 giugno 2001, n. 231
- GDPR 679/2016
- Decreto legislativo 21 novembre 2007, n. 231
- Circolare Banca d'Italia 285/2013 e successivi aggiornamenti

### Lezione II - Venerdì 10/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)

#### Fondamenti di Cybersecurity: Information Security Governance e ICT Compliance

- 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 III - Giovedì 16/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**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
  - Open Web Application Security Project (OWASP)
- Esercitazione:
  - Password cracking

**Lezione IV - Venerdì 17/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**Cybersecurity Risk Assessment: Contestualizzazione delle minacce – Business Impact Analysis**

- Risk analysis
  - Qualitativa, Semi-quantitativa e quantitativa
  - OCTAVE e altri metodi di analisi del rischio secondo la ISO 31000 e ISO/IEC 31010
- Risk Treatment
  - Trasferire, mitigare, accettare, evitare il rischio
- Impact Assessment
  - Business Impact Analysis secondo la ISO/TS 22317
- Esercitazione:
  - Realizzazione di una BIA

**Lezione V - Giovedì 23/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**Laboratorio di cyber security: nozioni tecniche avanzate**

- Tecniche di crittografia e Autenticazione
  - Crittografia simmetrica e asimmetrica;
  - Firma digitale (eIDAS)
- Cloud computing
  - IaaS, PaaS, SaaS
  - Caratteristiche di sicurezza di un protocollo per la gestione di transazioni finanziarie (es: pagamenti con carta)
    - Canali di comunicazione e sicurezza (es: TCP/IP, HTTPS con autenticazione TLS, altri)
    - Principali algoritmi crittografici per la cifratura del protocollo dati (es: TDES, AES, altri)
    - Modalità di autenticazione del protocollo dati (es: Hash, MAC, Digital Signature)
    - Esempi di implementazione
    - Normative e best practices di riferimento
- Case Study: OVH in fiamme
- Esercitazione:
  - Password safe (vault)
  - Messaggistica cifrata
  - Autenticazione e verifica di documenti e messaggi

**Lezione VI - Venerdì 24/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

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

- Case studies:
  - Stuxnet
  - Maersk
  - Solarwind
- Tecniche di Business Continuity / Disaster Recovery
  - Fail-over
  - Back-up and versioning systems (con tip & tricks)
- Esercitazione:
  - Phishing
  - Invio di email spoofing

**Lezione VII - Giovedì 30/06/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**Perimetro cibernetico nazionale: Standards e Best practices di riferimento della cybersecurity**

- Gli standard e le best-practice a supporto del Perimetro cibernetico Nazionale
- La struttura HLS delle ISO, ISO/IEC 27001 e ISO/IEC 27002
  - Struttura generale di una ISO
  - Elementi caratteristici della ISO/IEC 27001
  - I controlli della ISO/IEC 27002
  - Implementazione della ISO/IEC 27001 e altri standard (ISO/IEC 20000-1 o ITIL) secondo la ISO/IEC 27013
- NIST SP 800-53 e NIST Cybersecurity framework
  - Struttura NIST
  - Mappatura tra ISO/IEC e NIST
- Case Study:
  - Microsoft ISO/IEC 27001 Certification

**Lezione VIII - Venerdì 01/07/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**Security Convergence: L'importanza della sicurezza fisica nella sicurezza informatica**

- Fondamenti di sicurezza fisica e security convergence
- I controlli di sicurezza fisica nello standard ISO 27001 (A.11) e nella NIST 800-53
- Aree sicure
  - Il perimetro di sicurezza fisica e i controlli ai punti di entrata
  - Sicurezza degli uffici, stanze e altre strutture e protezione contro minacce esterne ed ambientali
- Attrezzature
- Case Study:
  - Protezione del datacenter nel bunker

**Lezione IX - Mercoledì 06/07/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**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

**Lezione X - Giovedì 07/07/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**Cybersecurity e processi di conformità: Consapevolezza di cybersecurity e competenze di cybersecurity**

- Formazione
  - Formazione verticale e orizzontale
  - Formazione continua
  - Best-practices di formazione
- Le principali certificazioni personali: SANS, ISACA, ISC2
  - Certificazioni Manageriali
  - Certificazioni Tecniche
  - Certificazioni per auditor
- Le competenze secondo la ISO/IEC 27021
  - Tecniche
  - Manageriali
  - Comunicazione
- Esercitazione:
  - Sviluppo di un Business Case per l'attivazione di un cybersecurity training/awareness program

**Lezione XI - Venerdì 08/07/2022 - Ore 15:00/19:15 (con 15 minuti di coffee break)**

**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
  - Documenti aziendali per la gestione e il controllo del sistema informativo previsti dalla Circolare 285
  - Presidio delle Esternalizzazioni ICT
- Il contributo della Compliance per le tematiche di Compliance ICT
  - Perimetro normativo di ICT Compliance
  - Il Processo di ICT Compliance

Le lezioni saranno registrate e a disposizione dei partecipanti sulla piattaforma MeliusForm, partner organizzativa che assicura altresì il coordinamento amministrativo e didattico.

Al link <https://www.meliusform.it/percorsi-formativi/cybersecurity-information-security/docenti> troverete i curricula dei docenti del Master.

Sulla base delle richieste dei partecipanti e su temi ritenuti di comune interesse che saranno individuati nel corso dell'iniziativa, potranno essere inserite nel programma delle testimonianze affidate ad esponenti di enti e di primarie realtà imprenditoriali.