

Oggetto: MASTER DI ALTA FORMAZIONE PROFESSIONALE DI SECONDO LIVELLO IN CYBERSECURITY MANAGEMENT

Salerno Formazione, società operante nel settore della didattica della formazione professionale certificata secondo le normative UNI ISO 21001:2019 + UNI EN ISO 9001:2015 settore EA 37 per la progettazione ed erogazione di servizi formativi in ambito professionale e Polo di Studio Universitario di Salerno dell'Università Telematica eCampus, organizza il MASTER DI ALTA FORMAZIONE PROFESSIONALE DI SECONDO LIVELLO IN CYBERSECURITY MANAGEMENT.

Il Master in Cybersecurity Management è un percorso formativo avanzato pensato per chi desidera acquisire competenze manageriali e tecniche nel campo della sicurezza informatica, oggi uno dei settori più strategici e richiesti dal mercato del lavoro.

In un contesto in cui le minacce digitali crescono in modo esponenziale, le aziende e le istituzioni necessitano di professionisti in grado di prevenire, gestire e mitigare i rischi informatici, garantendo la protezione dei dati, delle infrastrutture e dei processi aziendali.

Il Master in Cybersecurity Management rappresenta un investimento strategico per coloro che intendono assumere un ruolo centrale nella protezione delle informazioni e nella salvaguardia degli asset digitali delle organizzazioni.

Attraverso 11 moduli formativi e 55 capitoli di studio, il Master offre un approccio completo e multidisciplinare che integra:

- Competenze tecniche (reti, sistemi, cloud, crittografia, application security)
- Competenze gestionali (risk management, compliance, governance, strategie aziendali)
- Competenze operative (incident response, digital forensics, cyber threat intelligence)

I partecipanti impareranno a:

- ✓ Progettare e implementare strategie di sicurezza efficaci
- ✓ Definire politiche e procedure aziendali di cybersecurity
- ✓ Valutare e gestire rischi informatici complessi
- ✓ Rispondere a incidenti di sicurezza e coordinare team specializzati
- ✓ Anticipare le sfide future legate a nuove tecnologie e minacce emergenti

Il programma è rivolto a:

- Professionisti IT e Security Specialist che vogliono avanzare di carriera
- Manager e consulenti che desiderano specializzarsi nella gestione della sicurezza digitale
- Laureati interessati a entrare in un settore ad altissimo potenziale di crescita

Al termine del Master, i partecipanti saranno in grado di assumere ruoli di leadership come:

- ◆ Cybersecurity Manager
- ◆ Chief Information Security Officer (CISO)
- ◆ Risk & Compliance Specialist
- ◆ Incident Response Coordinator
- ◆ Security Consultant

DURATA E FREQUENZA: Il master avrà la durata complessiva di sei mesi. Il master si svolgerà presso la sede della Salerno Formazione con frequenza settimanale per circa n. 3 ore lezione.

È POSSIBILE SEGUIRE LE LEZIONI, OLTRE CHE IN AULA, ANCHE IN MODALITÀ E-LEARNING – ONLINE.

È prevista solo una quota d'iscrizione di € 500,00 per il rilascio del DIPLOMA DI MASTER DI ALTA FORMAZIONE PROFESSIONALE DI SECONDO LIVELLO IN CYBERSECURITY MANAGEMENT.

DESTINATARI: Il master è a numero chiuso ed è rivolto a n. 16 persone in possesso di laurea specialistica.

PROGRAMMA DI STUDIO:

Modulo 1 – Fondamenti di Cybersecurity

- Concetti base di sicurezza informatica
- Tipologie di minacce e vulnerabilità
- Modelli di sicurezza delle informazioni (CIA Triad)
- Standard e normative internazionali (ISO 27001, NIST, GDPR)
- Ruolo del Cybersecurity Manager

Modulo 2 – Reti e Infrastrutture Sicure

- Architettura delle reti e protocolli principali
- Firewall, IDS/IPS e sistemi di filtraggio
- Segmentazione e sicurezza delle VLAN
- Wireless Security e VPN
- Best practices per la sicurezza perimetrale

Modulo 3 – Sistemi Operativi e Sicurezza delle Piattaforme

- Sicurezza nei sistemi Windows
- Sicurezza nei sistemi Linux/Unix
- Gestione delle patch e aggiornamenti
- Hardening delle macchine e dei server
- Strumenti di monitoraggio e auditing

Modulo 4 – Sicurezza delle Applicazioni

- Ciclo di vita sicuro del software (SDLC)
- OWASP Top 10 e vulnerabilità comuni
- Tecniche di penetration testing sulle applicazioni web
- Sicurezza nelle API e nei microservizi
- Sicurezza delle app mobili

Modulo 5 – Criptografia e Protezione dei Dati

- Principi e storia della crittografia
- Crittografia simmetrica e asimmetrica
- PKI, certificati digitali e gestione delle chiavi
- Hashing e firma digitale

- Applicazioni pratiche della crittografia (SSL/TLS, VPN, e-mail)

Modulo 6 – Cyber Risk Management

- Identificazione e classificazione dei rischi
- Valutazione qualitativa e quantitativa
- Risk treatment: mitigazione, trasferimento, accettazione
- Business Continuity e Disaster Recovery
- Enterprise Risk Management e framework di riferimento

Modulo 7 – Cyber Threat Intelligence & Incident Response

- Modelli e fonti di Cyber Threat Intelligence (CTI)
- Indicatori di compromissione (IoC) e strumenti SIEM
- Incident Response Plan: fasi e procedure
- Digital Forensics: tecniche e strumenti
- Analisi di casi reali di incidenti informatici

Modulo 8 – Cloud & Virtualization Security

- Modelli di servizio e responsabilità condivisa (IaaS, PaaS, SaaS)
- Minacce e vulnerabilità nel cloud
- Sicurezza nei container e ambienti virtualizzati
- Compliance e certificazioni nel cloud (ISO, CSA, GDPR)
- Strumenti di monitoraggio e protezione in ambienti cloud

Modulo 9 – Cybersecurity Governance & Compliance

- Struttura e policy di sicurezza aziendale
- Conformità a GDPR, HIPAA, PCI-DSS
- Audit interni e certificazioni di sicurezza
- Security Awareness e formazione del personale
- Reporting alla direzione e stakeholder management

Modulo 10 – Cybersecurity in ambito Industriale e IoT

- Sicurezza dei sistemi SCADA e ICS
- Vulnerabilità e attacchi ai dispositivi IoT
- Strategie di protezione nelle smart cities
- Sicurezza in ambito sanitario e automotive
- Best practices per l'Industrial Cybersecurity

Modulo 11 – Strategie di Cybersecurity Management

- Pianificazione e sviluppo di una strategia di sicurezza aziendale
- Leadership e gestione dei team di sicurezza

- Budgeting e investimenti in cybersecurity
- Gestione della comunicazione in caso di crisi
- Trend futuri: AI, Quantum Computing e Cybersecurity del domani

Per ulteriori informazioni e/o per le iscrizioni, è possibile contattare dal lunedì al sabato dalle ore 9:00 alle 13:00 e dalle 16:00 alle 20:00 la segreteria studenti della Salerno Formazione ai seguenti recapiti telefonici 089.2097119 e/o 338.3304185 e/o WhatsApp: 392 677 3781.

SITO WEB: www.salernoformazione.com