MODULO A

FONDAMENTI DI CYBER SECURITY:

Competenze chiave per proteggere le informazioni e gestire i rischi digitali

Information Security & Cyber Risk Management

Scuola Internazionale ®
ETICA&SICUREZZA
MILANO - L'AQUILA

ICMQ

Finalità del corso

La cybersecurity non è solo un aspetto tecnico, ma un fattore strategico essenziale per la protezione del business. Il corso "Fondamenti di Cyber Security" offre una panorasca operativa per trasformare la sicurezza informatica da adempimento a leva competitiva. Progettato per professionisti IT, responsabili sicurezza e compliance, il percorso unisce teoria e pratica in 4 ore intensive, con focus su rischi digitali, controlli tecnologici e framework normativi. Attraverso simulazioni guidate, analisi di scenari reali e strumenti come SIEM, EDR e crittografia, i partecipanti impareranno a valutare vulnerabilità, implementare piani di remediation e integrare modelli ISO 27001/NIST. Un'occasione per acquisire competenze trasversali su threat intelligence, gestione incidenti e compliance GDPR/DORA, con un approccio concreto alla costruzione di sistemi resilienti.

I risultati attesi

I partecipanti acquisiranno strumenti operativi per:

- Identificare i rischi cyber nel contesto organizzativo
- Impostare e valutare controlli di sicurezza efficaci
- Applicare framework normativi (ISO 27000, NIST CSF, GDPR)
- Gestire incidenti e rafforzare la resilienza aziendale
- Integrare tecnologie come SIEM, EDR e crittografia

Destinatari

Professionisti IT, responsabili sicurezza, manager e personale operativo di ambito IT/Security/Compliance coinvolti nell'implementazione di programmi di cybersecurity.

Durata del corso e crediti

Il corso ha la durata di **4 ore** e consente di acquisire **4 crediti formativi** ai fini del mantenimento della certificazione dei professionisti della security certificati UNI 10459.

Metodologia

Il corso sarà erogato tramite **piattaforma e-learning** che permetterà lo scambio interattivo tra i partecipanti e i docenti coinvolti, favorendo lo scambio di idee, opinioni ed esperienze.

Per partecipare ai corsi FAD non occorrono particolari strumenti: è sufficiente una buona connessione ad internet ed un PC dotato di videocamera; la piattaforma interattiva per la gestione delle lezioni, **GoToMeeting, Zoom, Meet** e sarà comunicata successivamente e messa a disposizione da ICMQ. Una volta iscritti, riceverete una mail/calendar con il link per la connessione e l'orario. A questo punto, basterà cliccare sul link indicato, scaricare l'applicazione per accedere alla piattaforma e quindi al vostro corso. Materiale didattico fornito in formato elettronico.

Attestato

Al termine del corso verrà rilasciato un attestato di frequenza.
Con una frequenza di almeno il 95% del Corso e il superamento del test finale con un punteggio pari o superiore al 60% di risposte corrette verrà rilasciato l'attestato di partecipazione.

Programma e date del corso

9:00 – 9:15 Introduzione e presentazione

9:15 – 10:00 Introduzione alla Cybersecurity

- Sfide attuali e impatto business
- Asset informativi e classificazione dati
- Threat intelligence e scenario normativo (GDPR, NIS 2, DORA)

10:00 – 11:30 Controlli di Sicurezza e Tecnologie

- Strumenti avanzati: EDR, SIEM, firewall di nuova generazione
- Crittografia e Data Loss Prevention
- Vulnerability Assessment/Penetration Test

11:30 – 11:40 Coffee break

11:40 – 12:30 Governance e Framework

- ISO/IEC 27000 e NIST Cybersecurity Framework
- Modelli di maturity e Security Operation Center (SOC)
- Disaster Recovery e Business Continuity

12:30 – 12:50 Case Study Applicativo

- Analisi di un caso studio
- Definizione baseline sicurezza
- Piano di remediation per vulnerabilità critiche

12:50 – 13:00 Test di valutazione finale

Tutti i moduli del percorso cyber training

15 aprile 2025
Modulo A: FONDAMENTI DI CYBER SECURITY

16 aprile 2025
Modulo B: NIS2 READINESS

13 maggio 2025
Modulo C: BUSINESS CONTINUITY AND INCIDENT RESPONSE

14 maggio 2025
Modulo D: AI GOVERNANCE - ISO/IEC 42001:2023

Docenti

Daniele BAUDONE

Laureato in Informatica presso l'Università di Pisa, ho partecipato a start-up e collaborato con aziende e società di consulenza, in qualità di Business Unit Director, Consulente Cyber Security, Chief Information Security Officer, GRC Director svolgendo attività manageriali e consulenziali, di business development e di consulenza direzionale e tecnica.
Ho avviato e diretto team di ICT security in aziende multinazionali hi-tech/cloud, garantendo una gestione efficace della sicurezza informatica che ne ha supportato con successo gli obiettivi e la crescita.
Il mio obiettivo è trovare la corrispondenza più adeguata tra i requisiti di business e di sicurezza, perseguendo l'innovazione attraverso l'uso sicuro ed efficace delle ICT per abilitare il business e garantire l'affidabilità, aiutando le organizzazioni a migliorare la loro postura di sicurezza informatica.
Attualmente sono referente Senior in Scuola Internazionale Etica & Sicurezza per tutte i servizi di consulenza e formazione dell'area Information Security & Cyber Risk Management.