Innovazione digitale AI

Cybersecurity: protezione e sicurezza informatica

Fornire alle imprese competenze tecniche e operative per prevenire, rilevare e rispondere alle minacce informatiche, proteggendo dati, processi e infrastrutture aziendali. Il corso punta a sviluppare consapevolezza diffusa, capacità decisionali e autonomia nella gestione delle criticità cyber.

OBIETTIVI

- Comprendere il panorama delle minacce informatiche e i principali vettori di attacco.
- Saper identificare vulnerabilità nei processi, nelle persone e nei sistemi.
- Applicare politiche e procedure di sicurezza efficaci in azienda.
- Utilizzare strumenti operativi per la gestione sicura dei dati, delle reti e degli accessi.
- Conoscere le normative di riferimento (GDPR, misure minime di sicurezza).
- Saper costruire un piano di incident response e di continuità operativa.

DESTINATARI

Imprenditori, manager, responsabili IT, DPO, responsabili amministrativi, HR, personale operativo,consulenti e professionisti che utilizzano strumenti digitali o gestiscono dati sensibili.

DURATA e metodologia di erogazione

20 ore
Aula, Webinar; Esercitazioni pratiche, casi reali di aziende, simulazioni, utilizzo strumenti operativi e lavoro guidato su policy interne.

CONTENUTI

Modulo 1 — Introduzione alla Cybersecurity e ai rischi digitali

- Tipologie di minacce (phishing, malware, ransomware, social engineering).
- Impatti economici e organizzativi degli attacchi.
- Errori umani e vulnerabilità interne.

Modulo 2 — Sicurezza dei dati, degli accessi e dei dispositivi

- Best practice nella protezione dei sistemi.
- Gestione password e accessi privilegiati.
- Sicurezza cloud e mobile device management.
- Backup e crittografia.

Modulo 3 — GDPR, Data Protection e Sicurezza Organizzativa

- Ruoli e responsabilità (Titolare, Responsabile, Amministratore di Sistema).
- DPIA, misure tecniche e organizzative.
- Gestione documentale e data governance.

Modulo 4 — Incident Response e gestione operativa della sicurezza

- Identificazione attacchi, monitoraggio e segnalazioni.
- Procedure di risposta e contenimento.
- Business continuity e disaster recovery.

Laboratori pratici:

CyberLab – Attacchi e difese simulate:

- Analisi di un attacco ransomware.
- Simulazione phishing.
- Creazione piano minimo di difesa.
- Messa in sicurezza dispositivi e reti.

CERTIFICAZIONI RILASCIATE

Attestato di partecipazione

QUOTA DI ISCRIZIONE

Costo per partecipante € 300,00 + IVA
per gli associati al sistema Confindustria € 250,00 + IVA