CYBERSECURITY & RESILIENZA DIGITALE

Piano Formativo Strategico ex Direttiva NIS2, DORA e GDPR

01

Cyber Awareness & Phishing Simulation

PER TUTTI I DIPENDENTI E COLLABORATORI

Il firewall umano. Formazione pratica per la neutralizzazione delle minacce informatiche via email (Ransomware, BEC, Social Engineering). Erogazione di **campagne simulate di Phishing** per testare i riflessi della rete aziendale ed erogare formazione correttiva mirata.

02

Governance Cyber per il Board (NIS2 & DORA)

PER ORGANI DI GESTIONE, CDA E ALTA DIREZIONE

Assolvimento dell'obbligo formativo imposto ai vertici aziendali. Focus su **responsabilità legali, sanzioni amministrative e penali**, valutazione strategica del rischio cibernetico e procedure per l'approvazione delle misure di gestione e mitigazione delle minacce.

03

Gestione Incidenti & Crisis Management

PER CISO, DPO, RISK MANAGER E TEAM IT

Protocolli tecnico-giuridici di *Incident Response*. Gestione della continuità operativa (Business Continuity), mitigazione tecnica dell'impatto e tempistiche perimetrate per le **notifiche obbligatorie al CSIRT, ad ACN e al Garante Privacy (Data Breach)**.

04

Secure Coding & Supply Chain Risk

PER SVILUPPATORI, SOFTWARE HOUSE E COMPLIANCE

Integrazione della sicurezza *by design* (OWASP Top 10) nel ciclo di vita del software. Approfondimento sugli impatti del **Cybersecurity Act** sulla conformità dei prodotti digitali e tecniche di audit sul rischio cibernetico derivante dalla catena di fornitura ICT.

IL METODO EUCS: CYBER LEGAL ENGINEERING

- Approccio ibrido: competenze tecniche di **Cybersecurity** fuse con il rigore del **Diritto delle Nuove Tecnologie**.
- Analisi critica di **incidenti reali, Data Breach e ispezioni** delle Autorità di controllo.
- Erogazione del **Fascicolo di Compliance Formativa**: tracciamento degli accessi, verifica competenze e rilascio attestati.
- Programmi finanziabili al 100% attraverso i **Fondi Interprofessionali** per la competitività aziendale.

⚠ L'ERRORE UMANO È LA PRIMA VULNERABILITÀ DA CORREGGERE

Oltre il 90% degli attacchi ransomware va a segno a causa di un click errato. La mancata formazione del personale costituisce violazione delle Direttive europee, innesca la responsabilità diretta del management per

CULPA IN VIGILANDO

e aggrava in modo esponenziale l'esposizione sanzionatoria in caso di incidente informatico o Data Breach.