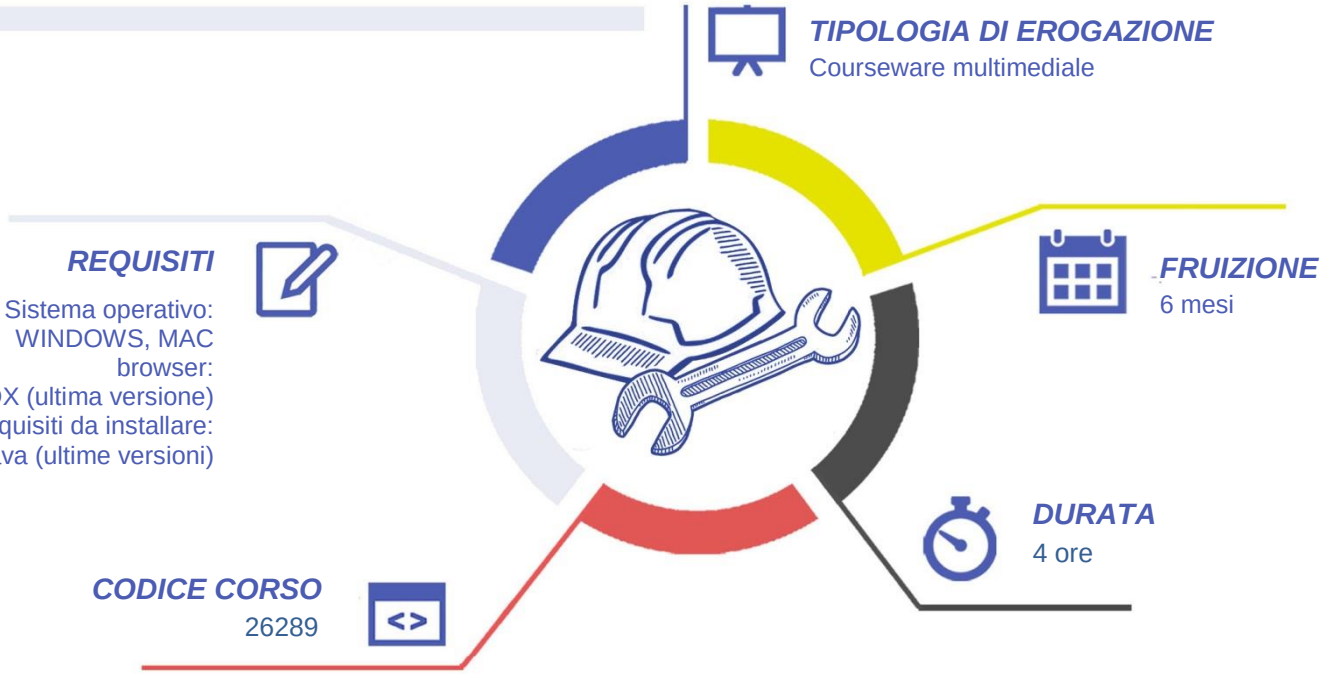
Cyber Security – Corso Base

A CHI SI RIVOLGE

Questo percorso è rivolto a tutto il personale che utilizza sistemi informatici durante la propria attività lavorativa.

OBIETTIVI

Rendere consapevoli i fruitori sul tema del cyber risk, che rappresenta un punto critico nel processo di analisi e riduzione dei rischi cui un'azienda può incorrere nella conduzione della propria attività. L'adozione di efficienti ed efficaci strumenti di gestione del cyber-rischio (cyber risk management) assume rilevanza cruciale, in quanto da essa possono dipendere le sorti stesse dell'impresa.



TIPOLOGIA DI EROGAZIONE
Courseware multimediale

REQUISITI
Sistema operativo:
WINDOWS, MAC
browser:
FIREFOX (ultima versione)
Requisiti da installare:
Java (ultime versioni)

FRUIZIONE
6 mesi

DURATA
4 ore

CODICE CORSO
26289

Interattiva editore

PERITI INDUSTRIALI

CONTENUTI

1. Aspetti generali
2. Sicurezza dei sistemi informatici aziendali e domestici
3. Le dimensioni della Cybersecurity
   3.1 Asset
   3.2 Threat (minaccia)
   3.3 Hacker & Cracker
   3.4 Bug weakness & vulnerability
   3.5Policy di sicurezza & Tool di protezione

4. Minacce comuni
4.1 Social Engineering e come difendersi.
4.2 Ransomware malware e spyware: Spyware, W orm, Ransomware, Attacchi attraverso la posta elettronica, Email e spoofing, Business Email Compromise (BEC), Gli attacchi ai devices mobili, I rischi delle reti Wi-Fi, La vulnerabilità dei siti web

5. Misure di sicurezza & integrità dei dati
   5.1 Parametri di Protezione
   5.2Sistemi di protezione: Cluster e ridondanza dei dati, Autenticazione e Password manager (Token, Sistema di riconoscimento biometrico, CAPTCHA, Metodi Crittografici, Protocollo 802.1x, Network Access Control, Virtual Private Network (VPN), Cookie, Gestioneutenti e relativi (policy utente), Firewall), Intrusion detection system (IDS), Network Intrusion Detection System (NIDS), Honeypot, Backup (Tipologie di backup, Supporti di memorizzazione, La gestione del repository, Manipolazione dei dati e la loro ottimizzazione), Antivirus (Antispyware, Steganografia, Firma digitale).

6.Il Framework Nazionale per la Cybersecurity
   6.1Imprese target del documento
   6.2Requisiti minimi
   6.3Controlli Essenziali di Cybersecurity: Controlli Essenziali di Cybersecurity,
   6.4 Applicazione dei controlli: Inventario dispositivi e software, Governance, Protezione da malware, Gestione password e account, Formazione e consapevolezza, Esempi di incidenti, Protezione dei dati, Protezione delle reti, Prevenzione e mitigazione. Sono trattati esempi di incidenti per ognuno dei controlli sopracitati

7. Raccomandazioni
   7.1Processo di sicurezza interno
   7.2Awareness e formazione
   7.3Filiere produttive e il processo di trasformazione digitale
   7.4Controllo, monitoraggio e valutazione delle vulnerabilità
   7.5Il rischio cyber all'attenzione dei vertici aziendali7.6Una certificazione leggera e dinamica per fornitori di servizi

TEST INTERMEDI

All'interno del corso vi sono dei momenti di verifica dell'apprendimento che consentono all'utente di interagire con l'animazione verificando l'apprendimento dei concetti presentati

SUPERAMENTO

Al termine del corso è previsto un test finale che verifica l'apprendimento con esercitazioni simili a quelle trovate nel corso riguardanti l'intero contenuto suddiviso per i moduli fruiti.

INDUSTRIA 4.0

Questo corso fa parte della formazione del "Piano Nazionale Impresa 4.0", grazie alla frequentazione del quale è possibile avere alcuni vantaggi (tra cui il credito d'imposta) previsti dal MiSE.

CERTIFICAZIONI

Il corso prevede il **rilascio di 7 Crediti Formativi Professionali** (CFP). Il corso è accreditato dal CNPI. L'attestato è rilasciato da Progetto Ulisse.

I VANTAGGI DELL'E-LEARNING

- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali
- Accessibilità ovunque e in ogni momento - Possibilità di rivedere le lezioni anche dopo aver terminato il corso