

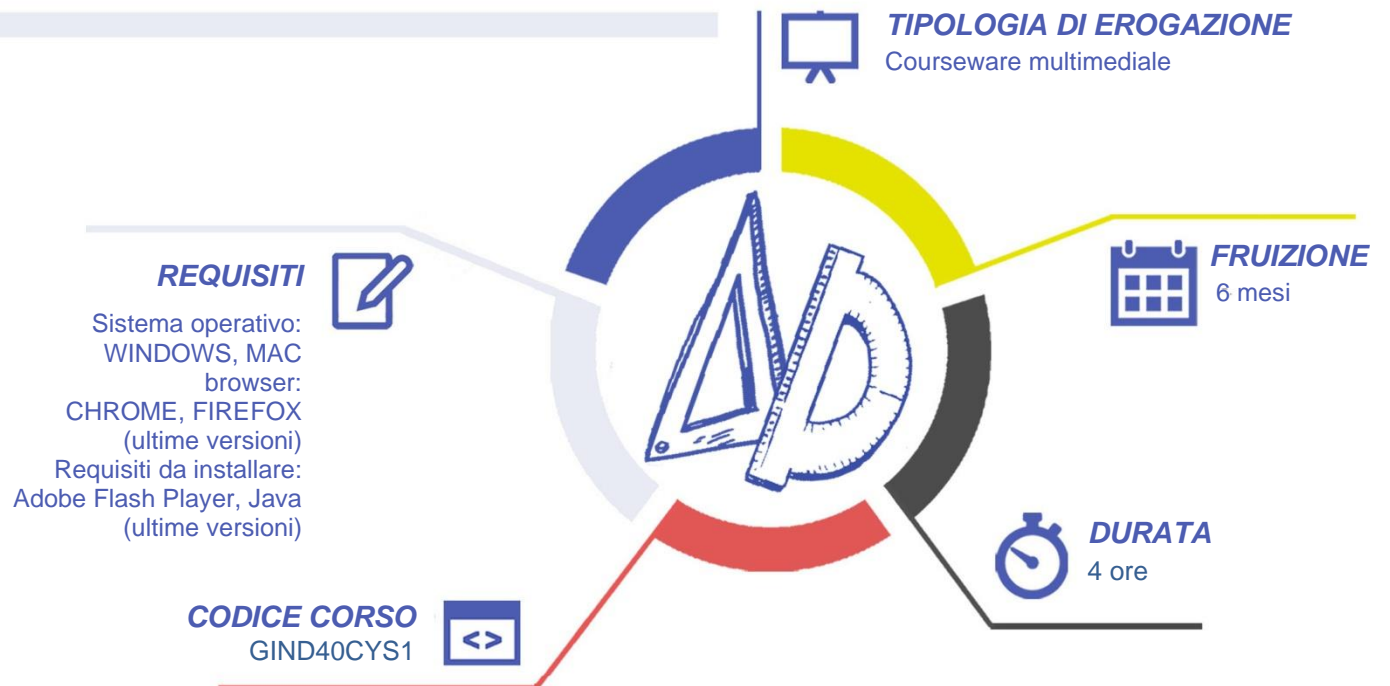
## Cyber Security – Corso Base

### 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.



# GEOMETRI

## 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
  - 3.5 Policy di sicurezza & Tool di protezione
4. Minacce comuni
  - 4.1 Social Engineering e come difendersi.
  - 4.2 Ransomware malware e spyware: Spyware, Worm, 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
  - 5.2 Sistemi 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, Gestione utenti 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
  - 6.1 Imprese target del documento
  - 6.2 Requisiti minimi
  - 6.3 Controlli 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
  - 7.1 Processo di sicurezza interno
  - 7.2 Awareness e formazione
  - 7.3 Filiere produttive e il processo di trasformazione digitale
  - 7.4 Controllo, monitoraggio e valutazione delle vulnerabilità
  - 7.5 Il rischio cyber all'attenzione dei vertici aziendali
  - 7.6 Una certificazione leggera e dinamica per fornitori di servizi

## TEST INTERMEDI

All'interno del corso vi sono dei momenti di verifica dell'apprendimento vincolati 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 domande a risposta singola e multipla riguardo l'intero contenuto del corso suddiviso per i moduli fruiti.

## CERTIFICAZIONI

Il corso è accreditato al CNG ed è valido al riconoscimento di 8 CFP.

## 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