

# CORSO INNOVAZIONE ORGANIZZATIVA E DI PROCESSO: CYBERSECURITY

Finanziato da Fondoprofessioni a valere su Avviso 4/2023



## DURATA e SEDE

Il corso ha durata di 24 ore realizzate in videoconferenza.

Le lezioni avranno cadenza settimanale per un impegno di 2 ore a settimana.



## DESTINATARI e REQUISITI DI ACCESSO

Il corso è rivolto a tutti i dipendenti delle Aziende / Studi aderenti al fondo Fondoprofessioni interessate alle iniziative promosse dagli Enti di Formazione proponenti.



## OBIETTIVI

Il progetto è finalizzato a promuovere la consapevolezza sulla sicurezza informatica e a fornire strumenti e strategie per gestire in modo efficace le minacce e le vulnerabilità nella gestione dei dati. Esplicitando gli obiettivi in dettaglio:

- ✓ Acquisire la conoscenza delle diverse minacce che possono compromettere la sicurezza dei dati, come gli attacchi informatici, il phishing, il malware e le violazioni della privacy.
- ✓ Acquisire le best practices per la gestione e la protezione dei dati sensibili dell'azienda e dei clienti, inclusa la crittografia, l'accesso sicuro e la gestione delle password.
- ✓ Apprendere come condurre un'analisi dei rischi per valutare l'impatto delle minacce sulla sicurezza dei dati e sviluppare strategie di mitigazione adeguate.
- ✓ Fornire linee guida sull'utilizzo sicuro di computer, telefoni cellulari, reti Wi-Fi e altri dispositivi aziendali e utilizzare software antivirus/antimalware.
- ✓ Rilevare, gestire e rispondere agli incidenti di sicurezza, compresa la segnalazione e la risoluzione delle vulnerabilità.
- ✓ Informare sui requisiti legali e regolamentari riguardanti la sicurezza informatica e su come l'azienda si adatta a tali normative.
- ✓ Comprendere il ruolo delle tecnologie emergenti



## PROGRAMMA

---

1. **Introduzione alla privacy** dei dati e alla cybersecurity: Introduzione alla privacy dei dati, concetti di base sulla protezione dei dati personali, normative e regolamenti sulla privacy (ad es. GDPR), principali minacce e rischi per la sicurezza dei dati.
2. **Analisi dei rischi e gestione della sicurezza dei dati**: Tecniche per l'analisi dei rischi, valutazione dell'impatto sulla sicurezza dei dati, identificazione delle vulnerabilità, classificazione degli asset critici, identificazione delle minacce e stime delle probabilità
3. **Normative e best practice per la privacy dei dati**: Principi fondamentali del GDPR, diritti degli interessati, obblighi del titolare del trattamento, ruolo del responsabile della protezione dei dati (RPD), best practice per la conformità normativa, gestione delle violazioni dei dati.
4. **Sicurezza informatica e protezione dei dati**: Tipologie di minacce informatiche (es. malware, phishing, attacchi DDoS), tecniche di protezione dei dati e dei sistemi (es. firewall, crittografia, autenticazione a due fattori), gestione delle vulnerabilità e degli accessi.
5. **Innovazione organizzativa per la cybersecurity**: Ruolo dell'innovazione organizzativa nella gestione della cybersecurity, sviluppo e implementazione di politiche e procedure interne, coinvolgimento dei dipendenti nella sicurezza dei dati, promozione di una cultura della sicurezza.
6. **Tecnologie emergenti e sfide della cybersecurity**: Ruolo delle tecnologie emergenti (es. intelligenza artificiale, cloud computing, Internet delle cose) nella cybersecurity, sfide e opportunità connesse, strategie di gestione dei rischi.



## COSTI E INFORMAZIONI

---

Il corso è **GRATUITO** in quanto finanziato da Fondoprofessioni.

Per informazioni ed iscrizioni: tel. 010 9861299 – [formazione@a-for.it](mailto:formazione@a-for.it)

