

# CORSO INNOVAZIONE ORGANIZZATIVA E DI PROCESSO: CYBERSECURITY PER GLI STUDI ODONTOIATRICI

Finanziato da Fondoprofessioni



## DURATA e SEDE

Il corso ha durata di 24 ore realizzate in videoconferenza.

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



## DESTINATARI e REQUISITI DI ACCESSO

Il corso è rivolto a tutti i dipendenti degli Studi Odontoiatrici aderenti al fondo Fondoprofessioni.



## OBIETTIVI

L'obiettivo principale di un corso di cybersecurity per gli studi odontoiatrici è creare una cultura di consapevolezza e sicurezza tra il personale, al fine di proteggere i dati dei pazienti e prevenire potenziali minacce informatiche.

Esplicitando gli obiettivi in dettaglio:

- ✓ Fornire una comprensione dettagliata delle minacce cibernetiche che possono interessare gli studi odontoiatrici, inclusi attacchi come ransomware, phishing e violazioni dei dati
- ✓ Mettere in evidenza l'importanza di proteggere i dati sensibili dei pazienti e fornire linee guida su come gestire in modo sicuro queste informazioni.
- ✓ Sensibilizzare il personale sugli aspetti chiave della sicurezza informatica
- ✓ Conoscere le procedure per l'accesso ai dati, la gestione delle password e la sicurezza fisica dei dispositivi informatici
- ✓ Saper gestire in modo sicuro le credenziali di accesso, promuovendo l'uso di password robuste e l'adozione di metodi di autenticazione a più fattori
- ✓ 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 lo studio si adatta a tali normative.



## PROGRAMMA

---

1. **Introduzione alla privacy e alla cybersecurity dei dati:** 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.



## 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)

