TIPOLOGIA EVENTO: WEB LIVE & E – LEARNING

PERCORSO CYBERSECURITY PER GLI STUDI PROFESSIONALI

Orario: 15:00 – 16:00 ***Durata: 2 ore***
Date: 06/05/2026 – 09/06/2026
Quota da listino: gratuito
Data di scadenza: 31/12/2026

CORPO DOCENTE

Mauro Muraca
Dottore Commercialista
Giulia Lansarotti
Esperta Product Marketing, Trust&Cyber

PROGRAMMA

I incontro - Le nuove minacce cyber per gli Studi professionali: rischi, protezione dei dati e buone pratiche

Evoluzione delle minacce cyber nel 2025–2026

- I nuovi trend degli attacchi informatici
- Perché gli studi professionali sono un bersaglio sempre più frequente
- Dati aggiornati sugli attacchi alle organizzazioni italiane

Protezione dei dati dei clienti

- Il valore delle informazioni gestite negli studi professionali
- I rischi legati alla perdita o alla compromissione dei dati
- Conseguenze operative, reputazionali e legali di un data breach

Le principali vulnerabilità negli studi professionali

- Sistemi non aggiornati e configurazioni errate
- Accessi condivisi e gestione non sicura delle credenziali
- Errori umani e mancanza di consapevolezza

Attacchi informatici negli studi: esempi concreti

- Phishing e furto di credenziali
- Ransomware e blocco dell'operatività dello Studio
- Accessi non autorizzati ai dati dei clienti

Migliorare la cyber consapevolezza nello Studio

- Buone pratiche di cyber igiene
- Il ruolo dei collaboratori nella sicurezza dello studio
- Come costruire una cultura della sicurezza informatica

Il incontro - Cyber risk management negli Studi Professionali: quantificare il rischio e proteggere la filiera digitale

Dal rischio informatico al rischio economico

- Quanto può costare realmente un attacco informatico
- Impatti operativi, economici e reputazionali per uno Studio
- Perché è importante misurare il rischio cyber

Quantificazione economica del rischio cyber

- Come stimare il potenziale danno di un attacco
- Dalla vulnerabilità all'impatto economico
- Il valore della misurazione del rischio nelle decisioni di sicurezza

Il rischio delle terze parti e della supply chain digitale

- Software, fornitori IT e servizi cloud
- Accessi ai sistemi dello studio da parte di terzi
- Come valutare i rischi legati ai fornitori

Cybersecurity e compliance

- Normative e responsabilità nella protezione dei dati
- L'importanza di un approccio strutturato alla sicurezza
- Strumenti per monitorare e gestire il rischio nel tempo