43

LEGALE E FISCALE

Durata
7 ore

Formazione a distanza
3 e 9 febbraio - mattino
12 e 19 marzo - mattino
2 e 9 aprile - mattino
9 e 15 giugno - mattino

Quota di partecipazione
250,00 € + IVA az. associate
300,00 € + IVA az. non associate

Iscrizione
Vedi le modalità alle pagine 4 e 5

CYBERSECURITY: IL PUNTO DEBOLE È IL FATTORE UMANO

Per una difesa efficace, la tecnologia non è sufficiente: servono competenze, consapevolezza e formazione. Il fattore umano rappresenta infatti una delle principali vulnerabilità per la sicurezza informatica aziendale.

Obiettivi
Il corso intende rafforzare la conoscenza delle normative e delle principali minacce in materia di cybersecurity, offrendo strumenti pratici per riconoscere, prevenire e ridurre i rischi connessi all'utilizzo quotidiano delle tecnologie.
Attraverso esempi concreti, i partecipanti acquisiranno maggiore consapevolezza e buone pratiche per una gestione sicura dei dati e dei dispositivi.

Destinatari
- Tutto il personale aziendale che utilizza dispositivi per il trattamento dati (computer, tablet, smartphone, ecc.)
- Responsabili IT (1° livello)

Contenuti
- Il GDPR in pillole: principi fondamentali, le basi giuridiche dei trattamenti, le figure coinvolte (Interessati, Titolare, Addetto, ecc...), i diritti degli interessati, la circolazione delle informazioni nei paesi EU ed Extra EU
- Le misure di sicurezza tecniche ed organizzative per prevenire i rischi sulla Riservatezza, Integrità, Disponibilità e la resilienza
- Le minacce più comuni
- Tecniche e tipologie degli attacchi informatici
- Le principali minacce: i programmi pericolosi (virus, adware etc.)
- Utilizzo in sicurezza degli strumenti in dotazione al dipendente per lo svolgimento delle mansioni sul luogo di lavoro
- Posta Elettronica: il valore di procedure e regolamenti
- L'importanza delle password per la protezione del patrimonio informativo
- L'importanza dei back up e degli aggiornati di Sistemi Operativi (pc, dispositivi mobili)
- La scelta dei fornitori e la verifica dei contratti da sottoscrivere
- Cyber-mafia: la nuova frontiera della criminalità organizzata
- Un attacco che non attacca: da chi ci si deve difendere
- Come comportarsi nelle prime fasi in cui si è venuti a conoscenza di un attacco. Chi coinvolgere per la valutazione dei potenziali danni
- Il ruolo delle autorità competenti.
- Le misure di sicurezza in ottica di privacy by design e by default Art. 25
- L'analisi dei rischi: fondamentale un aggiornamento costante
- Data breach (violazioni), la notificazione delle violazioni Art. 33, 34 e la relativa valutazione
- Le violazioni: la storia di chi è stato attaccato e le conseguenze per i dati degli interessati
- I Provvedimenti dell'Autorità Garante
- Gli standard di riferimento (ISO 27001, 27701, ENISA)
- La formazione: lo strumento più utile per un'efficace difesa

Docente
Daniele Gombi, pluriennale esperienza nella consulenza in data protection e data continuity. Dal 2018 opera come Data Protection Officer per numerose aziende, supportandole negli adeguamenti normativi e nella cybersecurity. Tiene corsi e seminari su privacy, sicurezza informatica e compliance alle principali norme di riferimento.