45

LEGALE E FISCALE

Durata
7 ore

Formazione a distanza
14 e 21 febbraio – mattino
8 e 15 maggio – mattino
5 e 12 dicembre – 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 da sola non basta, servono professionisti, consapevolezza e formazione.
Il fattore umano rappresenta una delle maggiori vulnerabilità.

Obiettivi
Apprendere ed approfondire le proprie conoscenze delle normative inerenti i nuovi rischi e le minacce, la sicurezza informatica e più in generale la "cybersecurity". Il corso formativo fornirà informazioni, suggerimenti e consigli per conoscere, prevenire e ridurre quanto più possibile i rischi connessi al fattore umano nell'utilizzo delle tecnologie.

Destinatari
Responsabili IT (1°livello) e personale aziendale dotato di device per il trattamento dati (computer, tablet, smartphone ecc. ...).

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
Luca Di Leo, svolge servizi e consulenza privacy dal 2006, formazione continua ed approfondita in merito agli adempimenti del D.Lgs. n. 196/2003, del Reg. UE 2016/679, per la protezione e sicurezza dei dati, sia nel contesto normativo nazionale che europeo. Si occupa di implementazione ed audit nell'ambito dei sistemi di gestione qualità, sia di sistema che di processo. Ha conseguito diverse certificazioni e qualificazioni delle competenze riconosciute sia a carattere nazionale che internazionale. Specializzato in campo sanitario, pubblica amministrazione, organizzazioni private, marketing, cyber security e svolge attività di consulenza e audit nel settore pubblico e privato. Partecipa a tavole rotonde e gruppi di lavoro che si relazionano direttamente con lo staff del Garante per la protezione dei dati personali. Ricopre il ruolo di Data Protection Officer nel settore pubblico e privato.

Gombi Daniele, Data Protection Officer, con competenze certificate da Unicert e Accredia, Privacy Officer con competenze certificate da TUV Italia, Membro della consulta UNICT di Unione Industriali Parma, commissione sicurezza informatica e Lead Auditor 27001.