

Privacy e Cybersecurity

per titolari del trattamento e collaboratori, imprenditori,
manager, professionisti e consulenti

OBIETTIVI DEL CORSO

Il corso è concepito per offrire percorsi dedicati alle differenti tipologie di professionalità che concorrono alla composizione del quadro inerente alla Privacy e Cybersecurity odierno, costituito da manager, imprenditori, professionisti e consulenti, esperti dell'ambito legale o dell'ambito informatico. Per ciascuna di queste categorie è possibile selezionare un percorso dedicato. Il programma proposto è quindi modulare e concepito per vestire le differenti esigenze di quanti intendono seguire, a partire da un modulo BASE propedeutico per tutti, un percorso più mirato su aspetti e temi legati alla Governance ed alla gestione di impresa o di consulenza presso imprese, seguendo i moduli ulteriori sui rami dell'area MANAGEMENT

MODULO BASE

area management (4 ore)

• Scenari esterni e interni all'azienda • Analisi organizzazione Aziendale, dei sistemi informativi, dei software utilizzati • Connessioni • Supporto hardware: pc, tablet, smartphone (proprietà aziendale?) • Come impostare l'Assessment • La risorsa dato: chi gestisce e come il dato, come proteggerlo

area legale (4 ore)

• I tratti essenziali delle problematiche della sicurezza • Come l'esigenza di sicurezza è recepita nella disciplina del DPGR • I dati personali e i principi che ne regolano il trattamento • Le varie competenze e responsabilità • I principali adempimenti richiesti • La documentazione da predisporre • Compliance e protezione da insidie e minacce • Violazioni, reazione, resilienza e sanzioni: disciplina e prassi comportamentali

area IT (4 ore)

• Protezione dei dati by Design: dai principi Privacy al design di sistemi informatici • DPIA e requisiti per il Privacy by Design • Esempi e casi d'uso • Introduzione alla Cybersecurity • I domini della Cybersecurity • Tool base ed esempi d'uso

MODULO INTERMEDIO MANAGER

area management (6 ore)

• Organigramma • Mansionario • Chi fa? Cosa? Come? • Analisi sistemi informativi • Assessment, creare un questionario • Inventario • Il perimetro • La risorsa umana • dove si "annida" il dato • Come si gestisce • La parte burocratica e amministrativa • Il registro • I ruoli del GDPR

area legale (2 ore)

• I tratti essenziali delle problematiche della sicurezza • Come l'esigenza di sicurezza è recepita nella disciplina del DGPR • I dati personali • I principi che ne regolano il trattamento: trasparenza e minimizzazione • Le varie competenze e responsabilità • Titolare, contitolari, responsabili e incaricati • I principali adempimenti richiesti e la documentazione da predisporre • Le misure di sicurezza • Compliance e protezione da insidie e minacce • Violazioni, reazione, resilienza e sanzioni • Esame di alcuni casi di studio

area IT (2 ore)

• Cybersecurity e Risk Management per l'IT • Comprendere ed applicare in IT la CIA triad • Security control frameworks

MODULO AVANZATO MANAGER

area management (6 ore)

• Accesso, accessibilità e controllo • Password sicure • autenticazione a più fattori • Firewall • Virus/Antivirus • Mail / Phishing / Cryptolocker • PEC / SPID / SMART CARD • navigazione sicura • social • identità digitale • Backup e sua periodicità • Sicurezza e integrità del dato • Cloud • Darkweb • controllo da remoto • iot • alexa / echo / google

area legale (2 ore)

• I tratti essenziali delle problematiche della sicurezza • Come l'esigenza di sicurezza è recepita nella disciplina del DGPR • Gli ambiti materiali e territoriali del trattamento • I dati personali • Le basi giuridiche del trattamento. Il consenso • principi che ne regolano il trattamento: trasparenza e minimizzazione • Le varie competenze e responsabilità • Titolare, contitolari, responsabili e incaricati • I principali adempimenti richiesti • Compliance e protezione da insidie e minacce • La documentazione da predisporre • Le misure di sicurezza • Violazioni, reazione, resilienza e sanzioni: disciplina e prassi comportamentali • Esame di alcuni casi di studio • Prova di redazione informative

area IT (2 ore)

• Cybersecurity e Risk Management per l'IT • Comprendere ed applicare in IT la CIA triad • Security control frameworks

N. MINIMO PARTECIPANTI

Il corso si attiverà con un numero minimo di 10 partecipanti fino ad un massimo di 20.

CALENDARIO E COSTO

Base 12 ore: 5, 12, 19 febbraio 2021 ore 14-18 € 100,00

Intermedio 10 ore: 26 febbraio 2021 e 5, 12 marzo 2021 ore 14-18 € 180,00

Advanced 10 ore: 19, 26 marzo 2021 e 2 aprile 2021 ore 14-18 € 270,00

MODALITÀ DI SVOLGIMENTO: il corso si svolgerà in video conferenza con possibilità di interazione con il docente

MODALITÀ DI ISCRIZIONE: www.asev.it