Corso - 24/02/2026

Cyber Resilience Act (CRA) - Quadro Normativo, requisiti Tecnici e conformità

Formazione pratica sul Cyber Resilience Act: comprendere la normativa UE, applicare i requisiti tecnici e garantire la conformità dei prodotti digitali.

Obiettivi

- Comprendere l'ambito di applicazione, i principi e le disposizioni del CRA;
- Conoscere i requisiti tecnici essenziali e le modalità di valutazione della conformità;
- Integrare i requisiti del CRA nei processi aziendali di sviluppo sicuro, gestione delle vulnerabilità e documentazione tecnica;
- Definire ruoli e responsabilità interne per garantire una conformità continuativa.

Programma

Modulo 1 – Ambito di applicazione, figure chiave e valutazione della conformità

24 febbraio, dalle 9:00 alle 13:00 - Online

Introduzione al CRA e ambito di applicazione

· Strategia europea di cybersicurezza
· Introduzione al CRA, ambito ed esclusioni
· Prodotti esclusi dall'ambito
· Immissione sul mercato di prodotti legacy
· Disposizioni transitorie (Articolo 69)
· Sostituzione dei prodotti
· Definizioni ed esempi
· Timeline
· Concetto di marcatura CE / regole del nuovo approccio
· Relazioni con altri Regolamenti UE sui prodotti (MD, RED, ecc.)

Procedure di valutazione della conformità

· Requisiti comuni per i prodotti con elementi digitali (Articolo 7)
· Classificazione dei prodotti
· Criteri per prodotti importanti e critici
· Moduli per la valutazione di conformità
· Organismi notificati
· Presunzione di conformità / concetto di armonizzazione e stato della normazione
· Dichiarazione UE di conformità e marcatura CE
· Sorveglianza del mercato

Ruoli e obblighi

· Obblighi del fabbricante
· Obblighi di importatori e distributori
· Sanzioni

Modulo 2 – Sviluppo Sicuro e requisiti tecnici

10 marzo , dalle 9:00 alle 13:00 - Online

Progettazione Sicura

· Ciclo di vita dello sviluppo sicuro del prodotto (Allegato I, Parte I, Punto 1)

· Requisiti e tecniche di valutazione dei rischi

Requisiti Tecnici

· Requisiti essenziali di cybersicurezza (Allegato I, Parte I, Punto 2)

Requisiti di gestione delle vulnerabilità

· Processo di gestione delle vulnerabilità (Allegato I, Parte II)

· Processo per aggiornamenti e periodo di supporto

· Gestione degli incidenti

· Obblighi di segnalazione (Articolo 14)

Modulo 3 – Standard di riferimento, fascicolo tecnico e roadmap per la conformità

24 marzo, dalle 9:00 alle 13:00 - Online

Standard di riferimento attuali per il CRA

· Situazione relativa agli standard armonizzati

· Sintesi degli standard di supporto disponibili (IEC 62443-4-2/-4-1, ETSI 303 645, ISO 2700x, IEC 30111, IEC 29147)

Open Source

· Obblighi dei responsabili del software open-source

· Attestazione di sicurezza del software libero e open-source

· Rischi e gestione dell'open-source

Documentazione Tecnica

· Informazioni e istruzioni per l'utente (Allegato II)

· Documentazione tecnica (Allegato VII)

Conformità al CRA

· Linee guida per l'implementazione dei requisiti CRA

· Raccomandazioni

· Esempi

Ulteriori informazioni

- Sono previste scontistiche sull'acquisto di più partecipazioni.
- La quota di partecipazione è comprensiva di materiale didattico in formato digitale e attestato di partecipazione.
- Si intendono aziende associate quelle aderenti alle associazioni: ACIMAC, ACIMALL, AMAPLAST, FEDERTEC E UCIMA.

Destinatari

Il corso è pensato per responsabili tecnici, responsabili della conformità, uffici legali, team di sviluppo software, security manager, responsabili qualità.

Durata

12 ore

Quota di adesione:

600,00 € + IVA a persona per le aziende associate

750,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento

24/02/2026 09.00-13.00 - ONLINE

10/03/2026 09.00-13.00 - ONLINE

24/03/2026 09.00-13.00 - ONLINE