



WEBINAR

Il Cyber Resilience ACT: i nuovi requisiti di cyber sicurezza dei prodotti digitali, gli obblighi per i fabbricanti e gli aspetti tecnico-normativi

8 e 14 ottobre 2026 – 9:30-13:00

Il Cyber Resilience ACT (CRA) mira a salvaguardare i consumatori e le imprese che acquistano prodotti software o hardware con elementi digitali, introducendo nuovi requisiti essenziali di sicurezza in materia di cybersicurezza dei prodotti, il cui rispetto **sarà necessario ai fini della apposizione della marcatura CE di conformità** e la legittima immissione sul mercato dei prodotti.

Il CRA impone ai fabbricanti obblighi di progettazione e sviluppo che assicurino la cybersicurezza dei prodotti con elementi digitali, oltre che obblighi di gestione delle vulnerabilità informatiche durante tutto il ciclo di vita dei loro prodotti, per i quali dovranno essere assicurati nel tempo aggiornamenti di sicurezza tempestivi. Alcuni prodotti di particolare rilevanza per la cibersicurezza potrebbero dover essere sottoposti a una valutazione da parte di terzi da parte di un organismo notificato prima di essere venduti sul mercato dell'UE.

I principali obblighi introdotti dal CRA si applicheranno a decorrere dall'11 dicembre 2027, mentre gli obblighi di comunicazione si applicheranno a decorrere dall'11 settembre 2026.

Obiettivi

Il webinar si propone di esaminare compiutamente il quadro legale degli obblighi e delle responsabilità in materia di cybersicurezza in capo in particolare ai fabbricanti di prodotti con elementi digitali nonché di approfondire il quadro tecnico normativo e certificativo di riferimento.

Destinatari

Imprenditori, Direttori Tecnici, Responsabili Tecnici e di laboratorio, Addetti Uffici Tecnici, Product Manager, Responsabili sviluppo e innovazione di prodotto, Responsabili Legali.

Relatori

Avv. Claudio Gabriele - partner dello Studio Associato Oddo Lora Gabriele, con attività esclusivamente dedicata al settore responsabilità d'impresa connessa alla immissione sul mercato, importazione di prodotti nella UE.

Ing. Alessandro Candeloro - Cybersecurity auditor presso IMQ S.p.A., una delle principali realtà italiane nel settore della valutazione della conformità, attiva da oltre 70 anni in certificazione, prove e ispezioni di prodotto a

supporto delle principali direttive europee.

Durata e modalità di svolgimento

8 e 14 ottobre 2026 - Dalle ore 9:30 alle ore 13:00 – Live Webinar.

Modalità e quota di iscrizione

1. Quota di partecipazione:
Associato ANIE € 500,00+IVA – Non associato € 700,00+IVA
Dal secondo partecipante sconto del 50%.
2. Iscrizione: finalizzare l'iscrizione on-line selezionando la modalità di pagamento.
3. Pagamento: con carta di credito o con bonifico bancario su: CRÉDIT AGRICOLE ITALIA S.P.A - SEDE MILANO - IBAN: IT 64 J 062300 16270 00006782136.
Per pagamento con bonifico bancario inviare la distinta a formazione@anieservizintegrati.it e amministrazione@anieservizintegrati.it. **L'iscrizione si intende perfezionata con l'avvenuto pagamento.**
4. Successivamente saranno inviate le modalità di partecipazione al webinar.

PROGRAMMA

8 ottobre 2026 – 09.30-13.00 (Parte legale)

Il *Cyber Resilience Act*:

- Il campo di applicazione: definizione di prodotti con elementi digitali e prodotti esclusi;
- Relazione con gli altri Regolamenti UE di prodotto (md, red, lvd, sicurezza generale ecc.) e direttiva NIS 2;
- Termini di entrata in vigore; l'applicabilità dei requisiti essenziali di sicurezza – l'applicabilità degli obblighi di segnalazione delle vulnerabilità sfruttate e degli incidenti gravi
- L'immissione sul mercato di prodotti con elementi digitali
- Il concetto di vulnerabilità informatica: le vulnerabilità note, le vulnerabilità sfruttabili, le vulnerabilità attivamente sfruttate

Ruoli ed Obblighi degli operatori economici:

- Obblighi dei fabbricanti: obblighi di progettazione, fabbricazione e di identificazione e correzione delle vulnerabilità –
- Gli obblighi dei fabbricanti dei prodotti in relazione ai software liberi ed Open
- Gli obblighi dei gestori di software open source;
- Gli obblighi di segnalazione degli incidenti e delle vulnerabilità sfruttate
- Accenni agli obblighi di Importatori, distributori e rappresentanti autorizzati;
- Periodo di assistenza obbligatoria: criteri applicabili per la determinazione del periodo di assistenza



ANIE Servizi Integrati è una società di



14 ottobre 2026 - 09.30 -13.00 (Parte tecnica)

- Requisiti essenziali di Cyber sicurezza: I requisiti dei prodotti ed i requisiti per la gestione delle vulnerabilità;
- Le norme tecniche armonizzate
- Le procedure di valutazione della conformità
- Documentazione tecnica
- Informazioni e istruzioni per l'utilizzatore
- Il ruolo degli organismi notificati
- La presunzione legale di conformità, la vigilanza del mercato, le non conformità formali, il sistema sanzionatorio;