CYBERSECURITY E RESILIENZA OPERATIVA DIGITALE:

IL NUOVO FRAMEWORK NORMATIVO EUROPEO

Il percorso formativo esamina il nuovo quadro normativo europeo in materia di cybersecurity e resilienza operativa digitale, analizzando gli impatti concreti in ambito aziendale. Attraverso l'approfondimento dei tre pilastri fondamentali – Direttiva NIS 2, Regolamento DORA e Cyber Resilience Act - forniremo una visione completa del framework normativo, comprensivo delle linee guida attuative, dei regolamenti esecutivi e degli standard tecnici in continua evoluzione. Il nostro approccio mira a:

- *garantire un aggiornamento costante sulle novità normative*
- *semplificare la comprensione delle nuove norme*
- *offrire una sintesi efficace delle disposizioni chiave*
- *guidare nell'implementazione pratica degli adempimenti richiesti*

Modalità

Il presente percorso è stato suddiviso in n. 3 webinar di 2 ore ciascuno che verranno erogati tramite "Microsoft Teams" nel mese di maggio 2025. Nei mesi successivi proporremo ulteriori incontri di aggiornamento sulle tematiche in oggetto. Ogni webinar (o modulo) sarà fruibile anche singolarmente.

Destinatari

Legale, Compliance ICT, Risk Management, Internal Audit, CISO, CIO, DPO, Consulenti privacy, Consulenti ICT, Sicurezza informatica

Date e orari

webinar 1 (NIS2)*: mercoledì 7 maggio – dalle ore 9.00 alle 11.00*

webinar 2 (DORA)*: mercoledì 14 maggio – dalle ore 9.00 alle 11.00*

webinar 3 (CRA)*: lunedì 19 maggio – dalle ore 9.00 alle 11.00*

[PROGRAMMA ARGOMENTI]

CYBERSECURITY: GLI ORIENTAMENTI APPLICATIVI DI NIS2, DORA E CRA DAI REQUISITI TECNICI AGLI OBBLIGHI DI REPORTING

webinar 1 *(7 maggio 2025)*:

Direttiva NIS 2: casi di incidente "significativo" e misure di gestione dei rischi

- Evoluzione del quadro normativo sulla cybersecurity europea (NIS 2, DORA, CRA)
- Interrelazioni tra le normative sulla cybersecurity secondo gli Orientamenti della Commissione ai sensi dell'art. 4 della Direttiva NIS 2
- Regolamento di esecuzione (UE) 2024/2690 sulle modalità di applicazione della direttiva NIS 2 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cybersecurity
- Specificazione dei casi in cui un incidente è considerato significativo secondo la direttiva NIS 2. Analisi di casi operativi: compromissione di un servizio di cloud computing; violazione della sicurezza di un data center; incidenti che coinvolge un fornitore di servizi gestiti.

webinar 2 *(14 maggio 2025)*:

Regolamento DORA: nuovi modelli standard di registro delle informazioni

- Breve panoramica sugli aspetti più importanti del DORA
- Decisione delle Autorità di Vigilanza Europee (EBA, EIOPA, ESMA) sulla comunicazione di informazioni per la designazione dei fornitori terzi critici di servizi TIC. Applicazione pratica: rinegoziare i contratti con i fornitori critici; gestire i rischi di concentrazione; rispondere agli incidenti che coinvolgono un fornitore.
- Nuovi modelli standard di registro delle informazioni sui contratti dei fornitori terzi di servizi TIC come disposto dal Regolamento DORA (Regolamento di

esecuzione (UE) 2024/2956): esercitazione pratica sulla compilazione e sull'utilizzo dei diversi modelli.

- Best practice e materiali operativi: fornitura dei modelli standard di registro e del report sui test di esercitazione UE

webinar 3 *(19 maggio 2025)*:

Cyber Resilience Act: security by design dei prodotti digitali e marcatura CE

- Cyber Resilience Act: analisi degli obblighi di cybersecurity per i prodotti con elementi digitali
- Focus sugli obblighi dei fabbricanti: requisiti di sicurezza, gestione delle vulnerabilità, periodo di assistenza minimo e sistema di notifica di vulnerabilità e incidenti gravi
- Obblighi per importatori e distributori: verifica della conformità, marcatura CE e adempimenti in caso di cessazione dell'attività del fabbricante
- Analisi dei principali impatti organizzativi e operativi: best practice per l'implementazione coordinata degli obblighi
- **Case study**: come ottenere la marcatura CE
- Principali impatti sull'operatività

RELATORE

Avv. Giovanni CIANO

Avvocato del foro di Milano, titolare dello Studio Legale Ciano. Si occupa di diritto delle nuove tecnologie e cybersecurity. Assiste primarie aziende in ambito di compliance, contenzioso e transizione digitale. Autore del volume "Digital Services Act e Digital Markets Act. Guida Pratica per Professionisti e Aziende". Pubblica articoli e partecipa in qualità di relatore a incontri e convegni in ambito giuridico.

Quote di partecipazione al percorso di formazione

"CYBERSECURITY E RESILIENZA OPERATIVA DIGITALE:
IL NUOVO FRAMEWORK NORMATIVO EUROPEO"

1. Intero percorso (3 webinar): **Euro 600** + 22% IVA a partecipante

2. Un singolo webinar: **Euro 250** + 22% IVA a partecipante

Per iscrizioni e ulteriori informazioni Tel. 02.36577120

e-mail: informa@informabanca.it