

CORSO DORA: CAPIRE IL REGOLAMENTO E IMPOSTARE L'ADEGUAMENTO DELL'ENTE

Durata: 7 ore



PROGRAMMA

MODULO 1: IL QUADRO DORA

- Obiettivi e perimetro di applicazione
- Proporzionalità: regime semplificato e regime completo
- Rapporto con NIS2 e GDPR
- Norme tecniche europee di attuazione
- Il quadro italiano (D.Lgs. 23/2025): autorità di vigilanza e sanzioni, anche per le persone fisiche
- Gli intermediari ex 106 TUB, soggetti a DORA dal 1° gennaio 2027
- Evoluzioni in discussione a livello europeo

MODULO 2: PILASTRO 1, GOVERNANCE E GESTIONE DEL RISCHIO ICT

- Ruolo e responsabilità dell'organo di gestione, compreso l'obbligo di formazione
- Quadro di gestione del rischio ICT e strategia di resilienza operativa digitale
- Identificazione di asset e funzioni essenziali o importanti
- Protezione, prevenzione e individuazione
- Risposta e ripristino, continuità operativa ICT, backup
- Apprendimento, formazione e comunicazione

MODULO 3: PILASTRO 2, GESTIONE E NOTIFICA DEGLI INCIDENTI ICT

- Processo di gestione degli incidenti
- Classificazione degli incidenti e delle minacce significative
- Notifica degli incidenti gravi: contenuti e tempi
- Comunicazione verso clienti e controparti

MODULO 4: PILASTRO 3, TEST DI RESILIENZA OPERATIVA DIGITALE

- Programma di test proporzionato alle dimensioni dell'ente
- Tipologie di test
- Test avanzati basati sulle minacce (TLPT): chi è obbligato e chi no

CORSO DORA: CAPIRE IL REGOLAMENTO E IMPOSTARE L'ADEGUAMENTO DELL'ENTE

Durata: 7 ore



MODULO 5: PILASTRO 4, RISCHIO ICT DERIVANTE DA TERZE PARTI

- Principi e strategia di gestione dei fornitori ICT
- Registro delle informazioni
- Rischio di concentrazione
- Requisiti contrattuali e subappalto
- Strategie di uscita
- Vigilanza sui fornitori ICT critici

MODULO 6: PILASTRO 5, CONDIVISIONE DELLE INFORMAZIONI E PIANO D'AZIONE

- Accordi di condivisione delle informazioni sulle minacce informatiche
- Definizione delle priorità per l'adeguamento

CORSO DORA: CAPIRE IL REGOLAMENTO E IMPOSTARE L'ADEGUAMENTO DELL'ENTE

Durata: 7 ore



OVERVIEW DEL CORSO

Il Regolamento (UE) 2022/2554, noto come DORA (Digital Operational Resilience Act), si applica dal 17 gennaio 2025 a banche, assicurazioni, SIM, SGR, istituti di pagamento e di moneta elettronica e agli altri enti finanziari, e coinvolge anche i fornitori di servizi ICT che lavorano per loro. In Italia il D.Lgs. 23/2025 ha indicato le autorità di vigilanza e le sanzioni, che possono riguardare anche le persone fisiche, e ha esteso le regole agli intermediari finanziari ex art. 106 TUB dal 1° gennaio 2027.

Il corso segue i cinque pilastri del regolamento: governance e gestione del rischio ICT, incidenti, test di resilienza, fornitori terzi e condivisione delle informazioni sulle minacce. Per ognuno distingue cosa vale nel regime semplificato e cosa nel regime completo, mostra come costruire sui presidi già attivi per NIS2, GDPR o ISO 27001 e si chiude con un piano d'azione per l'adeguamento.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Membri dell'organo di gestione e direzione che approvano il quadro di gestione del rischio ICT e ne rispondono
- Compliance, risk manager e internal audit che devono verificare la conformità e integrare DORA nei presidi esistenti
- CIO, IT manager e CISO che devono tradurre i requisiti in processi, controlli, test e piani di continuità
- Responsabili acquisti e outsourcing che gestiscono contratti, registro delle informazioni e strategie di uscita
- Fornitori di servizi ICT per il settore finanziario e intermediari ex art. 106 TUB

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Capire se DORA si applica alla propria organizzazione, con quale regime e con quali autorità e sanzioni
- Definire ruolo e responsabilità dell'organo di gestione e impostare il quadro di gestione del rischio ICT
- Identificare le funzioni essenziali o importanti e gli asset ICT che le supportano
- Impostare il processo di gestione, classificazione e notifica degli incidenti ICT gravi
- Costruire un programma di test proporzionato e capire se l'ente è tenuto ai test TLPT
- Gestire i fornitori ICT: registro delle informazioni, contratti, concentrazione e strategie di uscita
- Stabilire le priorità per l'adeguamento in un piano d'azione