

LA RESILIENZA OPERATIVA DIGITALE (DORA), RTS E ITS

10 e 12 ottobre 2023

1

Con la diffusione della digitalizzazione e dei servizi ad essa collegati i settori finanziario e fintech devono attrezzarsi e imparare a reagire tempestivamente alle minacce in continuo aumento rappresentate, fra gli altri, dagli attacchi informatici.

Nel mese di dicembre scorso sono state pubblicate nella Gazzetta Ufficiale UE:

- **il Regolamento DORA** (*Digital Operational Resilience Act*) **per la difesa unica europea** che ha l'obiettivo di disciplinare in maniera uniforme la "resilienza operativa" nel settore finanziario in tutta l'Europa.
- la **Direttiva DORA**
- ed anche la **NIS2**

Nei prossimi mesi saranno emessi una serie di documenti tecnici, a completamento di DORA (i primi sono stati emessi in consultazione a giugno 2023).

Tali normative impatteranno con le loro regole sull'intero ecosistema finanziario a prescindere dalle dimensioni e dal fatturato delle aziende e dei loro fornitori. Nel processo di adeguamento alla cyber resilienza saranno coinvolti direttamente i vertici aziendali. La gestione del rischio, gli obblighi di segnalazione, l'esecuzione di test di resilienza e la condivisione di dati comporteranno obblighi più rigorosi e severi. Il focus della normativa riguarderà anche la gestione dei rischi ICT derivanti da terze parti e i fornitori sono direttamente coinvolti per il rispetto delle nuove disposizioni.

Banche, Assicurazioni, operatori fintech e gestori di crypto-asset e tutti i relativi fornitori ed outsourcer dovranno **adeguarsi ai nuovi requisiti entro dicembre 2024** e sarà fondamentale evitare ritardi. DORA, accanto ad alcuni elementi di novità quali la vigilanza centralizzata sui fornitori, armonizza una serie di adempimenti già previsti da altre normative. L'impegno richiesto per la sua implementazione è quindi legato al settore di appartenenza delle singole organizzazioni e alla loro conformità alle normative già in vigore.

Il presente corso, molto pratico, si prefigge non solo di presentare quali sono gli adempimenti previsti da DORA, ma anche i possibili riferimenti (normativi, framework,

buone pratiche...) utilizzabili per una corretta implementazione anche alla luce del contenuto dei documenti tecnici fino ad ora disponibili.

[PROGRAMMA]

(* Ore 8.45 prova collegamento – ore 9.00 apertura dei lavori

2

La resilienza operativa nella normativa e la sua evoluzione

- Dalla continuità operativa alla resilienza operativa, differenze e sinergie
- L'iter legislativo di DORA, la strutturazione della norma, gli RTS
- Il perimetro di applicazione della normativa
- Le normative sulla resilienza al di fuori della UE

I pillar di DORA: analisi degli impatti e alcune utili indicazioni operative

- La gestione dei rischi informatici
- La gestione, classificazione e segnalazione degli incidenti informatici
- I test di resilienza operativa digitale
- La gestione dei rischi derivanti da terzi
- La condivisione delle informazioni

L'interazione con le altre normative

Le sanzioni

Esternalizzazioni e normativa

- Cloud e normativa
- La valutazione di un fornitore in cloud
- La definizione delle strategie di uscita

Gli RTS emessi a giugno 2023

- RTS sul Framework per la Gestione dei Rischi ICT (art. 15)
- RTS sul Framework semplificato per la Gestione dei Rischi ICT (art. 16)
- RTS sui criteri per la Classificazione degli Incidenti connessi all'ICT (art. 18.3)
- RTS per specificare la Politica relativa ai Servizi ICT offerti da Fornitori Terzi di Servizi ICT (art. 28.10)
- ITS per stabilire i modelli per il Registro delle Informazioni (art. 28.9).

Ore 13.00 chiusura dei lavori

(* Il corso si svolgerà nell'arco di due mattine (10 e 12/10/2023) con gli stessi orari

RELATORE: **Giancarlo BUTTI**

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Membro del Comitato Scientifico del CLUSIT (referente ESG ed Inclusion). Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy; affianca all'attività professionale a quella di divulgatore. Oltre 170 corsi, seminari e master universitari presso ISACA, CLUSIT, ITER, CETIF, IKN, AIIA, UNIVERSITA DI MILANO, POLITECNICO DI MILANO, UNIVERSITÀ DEGLI STUDI SUOR ORSOLA BENINCASA NAPOLI, CEFRIEL, UNISEF,... Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate, 26 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha inoltre partecipato alla redazione di 27 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT... Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di DFA (Digital Forensics Alumni) e del BCI (Business Continuity Institute), partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni: LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

3

Quota di partecipazione

comprensiva di materiale didattico su formato elettronico:

Euro 600 + 22% Iva a partecipante

Plus: a tutti i partecipanti verrà fornito (già compreso nella quota di iscrizione) il volume "Manuale di resilienza – Guida pratica alla progettazione gestione e verifica delle soluzioni di resilienza operativa, business continuity e disaster recovery"

Autore: **Giancarlo BUTTI**

N. di pagine: 600

Per iscrizioni e ulteriori informazioni Tel. 02/36577120 - email: informa@informabanca.it

Le informazioni sulle modalità di collegamento alla videoconferenza verranno fornite al partecipante al momento dell'iscrizione