Banca Ifis

DORA in avanti

Laura Quaroni
Resp. Privacy & Security Banca Ifis

28 maggio 2025

La normativa DORA è stata introdotta dall'Unione Europea per garantire che le istituzioni finanziarie siano preparate a gestire i rischi operativi e le minacce digitali

Banca Ifis

In un'epoca in cui la tecnologia svolge un ruolo cruciale nei servizi finanziari, DORA (Digital Operational Resilience Act) si presenta come un **framework normativo innovativo che affronta i rischi operativi, le minacce cyber e gli incidenti critici** con l'obiettivo di garantire resilienza e reattività delle organizzazioni alle minacce emergenti.

L'implementazione di DORA presenta diverse sfide significative, tra cui:

La **complessità della normativa**

La necessità di **adeguarsi rapidamente**

In risposta a tale contesto, Banca Ifis ha deciso di attivarsi anticipatamente e **svolgere, già nel 2023, un primo assessment** al fine di valutare il proprio posizionamento rispetto alla normativa. Nell'ultimo anno, sono stati realizzati **progetti al fine di rafforzare i processi e le procedure richiamate da DORA**.

Data la magnitudo della normativa si prevede, inoltre, che gli **argomenti trattati in DORA si evolveranno anche nel prossimo futuro** fornendo maggiori dettagli su come gestire concretamente la resilienza operativa.

L’applicazione della normativa DORA presenta sfide interpretative e realizzative

Banca Ifis

Interpretazione della normativa

La normativa **non fornisce dettagli precisi sulle caratteristiche di alcuni concetti lasciando spazio all’interpretazione della norma**.

Ad esempio non viene specificato a che livello identificare le **“critical important functions - CIF”,** oppure gli **“incident ICT related”.**

Classificazione degli incidenti

Le **soglie di classificazione degli incidenti** sono definite con driver più precisi, sia per incidenti ordinari che per quelli significativi.

Le entità finanziarie possono comunque **definire propri algoritmi modificando il peso da attribuire a ciascun driver**.

Test di sicurezza

La normativa prevede che le entità finanziarie **sottopongano i propri sistemi a test avanzati di resilienza operativa digitale**, ma permane una certa **ambiguità rispetto alla concreta definizione dei requisiti minimi richiesti.**

Ad esempio non sono forniti criteri uniformi **per calibrare la profondità e l’estensione dei test**, generando potenziali disallineamenti tra soggetti vigilati.

Principio di proporzionalità e framework normativi

Il framework delineato da DORA potrebbe risultare **sproporzionato in termini economici, organizzativi e tecnologici** soprattutto per le micro-imprese.

Inoltre, **l’assenza di integrazione o di mutuo riconoscimento tra altri framework normativi o di testing** (es. TIBER, linee guida EBA, ESMA, etc.) può determinare una duplicazione degli oneri operativi e documentali.

In particolare DORA ha influenzato vari aspetti relativi al processo di gestione degli incidenti

L'Incident Response è uno degli **ambiti chiave influenzati dal Regolamento DORA**, che ha avuto impatto e ha introdotto nuovi requisiti su:

- Formalizzazione e strutturazione della **risposta agli incidenti**
- Obbligo di **segnalazione degli incidenti ICT gravi**
- **Coordinamento interno ed esterno**
- **Simulazioni e test periodici**
- Coinvolgimento dei **fornitori ICT critici**

Banca Ifis ha **ottimizzato il processo di gestione degli incidenti,** definendo **logiche gestionali comuni e condivise** per le diverse tipologie di incidenti, creando **sinergie tra le competenze specialistiche dei diversi ambiti** e **ridisegnando le configurazioni degli strumenti tecnologici** a supporto della gestione degli incidenti.

La necessità di mantenere la **conformità del processo** anche su altri fronti (285, GDPR, PSD2, etc.) **ha reso complessa l'attività di integrazione in ottica DORA**, interessando tutti i componenti di processo:

persone *attività* *strumenti*

Grazie per l’attenzione!