Martedì 11 Febbraio 2025
Notizie [1]

Regolamento DORA e imprese

Sicuro non riguardi anche la tua?

Il **Regolamento DORA** [2] (Digital Operational Resilience Act) è una **normativa dell'Unione Europea** che mira a rafforzare la resilienza operativa digitale delle istituzioni finanziarie, come banche, assicurazioni e altre entità finanziarie, ma anche delle imprese che operano nel settore dei servizi finanziari.

L'obiettivo principale di DORA è quello di garantire che tutti questi soggetti siano **in grado di mantenere operazioni sicure e continuative**, anche in caso di attacchi informatici, guasti tecnologici o altre crisi digitali.

Scopriamo insieme **cosa prevede il regolamento** e, se rientri tra i suoi destinatari, **come adeguare la tua attività**.

Cosa prevede il regolamento DORA

Regolamento DORA e imprese. Prima di capire se può riguardare anche la tua attività, partiamo col dire che Il regolamento europeo DORA è entrato in vigore il 16 gennaio 2023 e si applica a partire dal 17 gennaio 2025. Le imprese devono rispettare le nuove normative entro il 2025, con scadenze specifiche per la gestione dei rischi e la segnalazione degli incidenti.

Dopo aver affrontato il tema della Direttiva NIS [3], le imprese devono ora prepararsi al più presto secondo quanto previsto da DORA, per evitare sanzioni o problematiche operative in futuro. Cosa devono fare le attività coinvolte? Ecco i punti salienti.

- **Gestione dei rischi ICT (Information and Communication Technology)**

Le attività devono identificare, monitorare e mitigare i rischi legati alle tecnologie informatiche. Questo include la gestione dei rischi relativi a software, infrastrutture, dati e reti di comunicazione.

- **Incidenti di sicurezza informatica**
  DORA impone alle istituzioni finanziarie di segnalare rapidamente incidenti di sicurezza informatica alle autorità competenti. La segnalazione deve avvenire entro 24 ore dal rilevamento dell'incidente.

- **Test di resilienza digitale**
  Le imprese devono condurre regolarmente test per garantire che i loro sistemi ICT siano in grado di resistere a crisi o attacchi informatici. Questi test devono essere documentati e i risultati devono essere valutati.

- **Gestione dei fornitori di servizi esterni**
  DORA obbliga le imprese a monitorare e gestire i rischi derivanti dai fornitori esterni di servizi ICT. Se un fornitore di servizi critici va in crisi, l'impresa deve avere piani di continuità operativa per evitare interruzioni dei servizi.

- **Piani di continuità operativa**
  Le imprese devono sviluppare e mantenere piani di continuità operativa e di recupero dei dati in caso di guasti o attacchi informatici.

- **Monitoraggio dei rischi a livello di sistema**
  DORA promuove un monitoraggio a livello di sistema, che consente alle autorità competenti di osservare la resilienza digitale complessiva del settore finanziario.

Regolamento DORA e imprese: chi sono i soggetti obbligati?

Il regolamento DORA impone obblighi principalmente alle istituzioni finanziarie, ai fornitori di servizi ICT critici e alle infrastrutture di mercato, ma si estende anche ad altre entità che hanno un impatto diretto sulla resilienza operativa digitale del sistema finanziario.

I **soggetti obbligati a recepire il regolamento DORA** sono:

1. Entità finanziarie

- **Banche** - soggetti che operano come intermediari finanziari e forniscono servizi bancari, come prestiti, depositi, pagamenti, ecc.

- **Assicurazioni e riassicurazioni** - compagnie di assicurazione che offrono polizze di vita, salute e danni, insieme ai riassicuratori.

- **Fondi pensione** - istituzioni che gestiscono fondi pensione, sia per il settore pubblico che per quello privato.

- **Gestori di fondi** - società che gestiscono fondi di investimento, come fondi comuni e fondi hedge.

- **Società di investimento** - attività che forniscono servizi di investimento, come la consulenza, la gestione di portafogli, la negoziazione di strumenti finanziari, ecc.

- **Borse e sistemi di pagamento** - piattaforme di scambio di strumenti finanziari e sistemi di pagamento.

- **Infrastrutture di mercato** - attività che operano come centri di compensazione, depositari centrali, camere di compensazione e altri sistemi che gestiscono transazioni finanziarie.

2. Fornitori di servizi ICT

- **Fornitori esterni di tecnologia e servizi digitali -** attività che forniscono software, infrastrutture cloud, soluzioni di cyber sicurezza, supporto tecnico e altri servizi ICT cruciali per il settore finanziario. Questi soggetti sono anch'essi soggetti a obblighi di conformità in relazione alla loro capacità di garantire continuità e sicurezza operativa.

- **Outsourcer tecnologici** - aziende che forniscono supporto esterno o outsourcing per la gestione dei sistemi informatici delle istituzioni finanziarie.

3. Infrastrutture critiche

- **Attività che forniscono servizi critici per il sistema finanziario** - tutti quei fornitori di servizi ICT che sono essenziali per il buon funzionamento delle istituzioni finanziarie e che possono essere considerati a rischio di interrompere la stabilità operativa del settore se i loro sistemi crollano o vengono compromessi.

4. Altri soggetti

- **Attività regolamentate dalla normativa europea sui mercati finanziari** - oltre alle istituzioni che gestiscono direttamente i servizi finanziari, il regolamento si applica anche a soggetti che sono regolamentati da altre normative europee e che svolgono funzioni critiche per il sistema finanziario;

- **Attività di vigilanza e regolamentazione** - le autorità di regolamentazione, come le autorità nazionali competenti e le autorità europee, sono coinvolte nel monitoraggio della conformità delle entità al regolamento.

Regolamento DORA e imprese. Come adeguare la tua attività alla normativa

La tua attività rientra tra quelle sopra elencate e quindi cade sotto l’ambito di applicazione di DORA? Se la risposta è sì, allora è necessario **intraprendere diversi passi per essere conforme al regolamento**:

1. **Valutazione del rischio ICT**
   Effettuare una valutazione approfondita dei rischi ICT associati alle tue operazioni, identificando vulnerabilità nei sistemi digitali e adottando misure per mitigarle.

2. **Implementazione di politiche di gestione del rischio digitale**
   Creare politiche interne per la gestione dei rischi informatici, che includano misure per prevenire, monitorare e rispondere agli incidenti.

3. **Formazione del personale**
   È fondamentale formare i tuoi dipendenti sulle best practices di sicurezza informatica e sulle procedure da seguire in caso di incidenti di sicurezza.

4. **Revisione dei contratti con i fornitori**
   Esaminare i contratti con i fornitori di servizi ICT per garantire che questi ultimi rispettino gli obblighi di resilienza digitale, prevedendo misure per monitorare e intervenire in caso di criticità legate ai fornitori.

5. **Piani di risposta agli incidenti**
   Stabilire e testare regolarmente piani di risposta a incidenti informatici, che comprendano la gestione della crisi e la comunicazione alle autorità competenti.

6. **Test periodici di resilienza digitale**
   Condurre test di resilienza digitale, come simulazioni di attacchi informatici e guasti tecnologici, per verificare la capacità di risposta dei loro sistemi.

7. **Compliance con le autorità nazionali**
   In Italia, la **Banca d'Italia** è l'autorità competente per supervisionare l'applicazione di DORA nel settore bancario e finanziario. La tua attività deve necessariamente collaborare con le autorità nazionali, comunicando tempestivamente gli incidenti di sicurezza e le vulnerabilità.

Regolamento DORA e imprese: inizia a difenderti da qui

Il regolamento DORA (Digital Operational Resilience Act) dell'UE mira a rafforzare la resilienza operativa digitale delle attività del settore finanziario. **Anche se non rientri tra le imprese obbligate a rispettare questo regolamento**, avviare un percorso di consapevolezza sui rischi informatici è importante per proteggere il futuro della tua attività.

Ti stai chiedendo come fare? Potresti rivolgerti alla Camera di commercio del tuo territorio.

Se sei alle prime armi in tema di cybersecurity, a disposizione della tua impresa ci sono **consulenze e servizi per aiutarti ad imboccare la strada corretta** attraverso i **Punti Impresa Digitali** [4] che mettono a tua disposizione soluzioni che vanno dalla formazione al mentoring. E proprio in tema sicurezza, puoi chiedere aiuto al PID col servizio **Cyber Check** [5]
Ultima modifica: Martedì 11 Febbraio 2025

Condividi

Reti Sociali

Gradimento Select rating Nessun voto

Rate

ARGOMENTI

Source URL: https://me.camcom.it/notizie/regolamento-dora-imprese

Collegamenti
[1] https://me.camcom.it/notizie/%3Ffield_notizia_categoria_tid%3D385
[2] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[3] https://www.cybersecurity-pmi.infocamere.it/notizie/direttiva-nis2-sicurezza
[4] https://www.cybersecurity-pmi.infocamere.it/notizie/digitalizzazione-pmi
[5] https://www.cybersecurityosservatorio.it/Services/PIDCyberCheck.jsp?lang=it