INSIGHT | 5 dicembre 2024

DORA: il framework di gestione dei rischi informatici per fornitori di servizi di crowdfunding

In vista dell'entrata in vigore del Regolamento Digital Operation Resilience Act (DORA) a partire dal prossimo 17 gennaio, riteniamo utile fare chiarezza sui principali obblighi previsti per i fornitori di servizi di crowdfunding. L'obiettivo di DORA, infatti, è quello di garantire un livello uniforme di resilienza operativa digitale, stabilendo regole precise in merito alla sicurezza dei sistemi informatici e delle reti che supportano i processi delle entità finanziarie.

I principali obblighi sono i seguenti:

1. **Gestione dei rischi informatici**: è richiesto che le entità predispongano un quadro di gestione e controllo interno ("**Framework**") in grado di garantire una gestione prudente ed efficace dei rischi informatici.

2. **Segnalazione degli incidenti**: le autorità competenti devono essere informate in caso di incidenti gravi legati alle tecnologie informatiche e di rete (TIC). Inoltre, è prevista la possibilità di segnalare volontariamente eventuali minacce informatiche significative.

3. **Contratti con fornitori di servizi TIC**: vengono stabiliti obblighi riguardanti gli accordi contrattuali tra le entità finanziarie e i fornitori terzi di servizi tecnologici.

4. **Registro degli accordi contrattuali**: è necessario mantenere un registro delle informazioni relative a tutti gli accordi stipulati con fornitori di servizi ICT terzi.

È importante sottolineare che DORA prevede un regime semplificato per gli intermediari di piccole dimensioni, come stabilito dall'articolo 16, comma 1 del regolamento, ma i fornitori di servizi di crowdfunding non rientrano tra questi soggetti.

Per garantire una corretta applicazione del regolamento, quest'ultimo prevede l'applicazione del principio di proporzionalità, ai sensi del quale si deve tenere conto delle dimensioni, del profilo di rischio, e della complessità dei servizi e delle attività svolte da ciascun soggetto obbligato. Pertanto, gli intermediari di dimensioni più piccole o con minori interconnessioni con il sistema, dovranno comunque rispettare gli obblighi, ma in maniera meno rigida e stringente.

Un aspetto importante per i fornitori di servizi di crowdfunding è rappresentato dagli esoneri previsti per le "microimprese", ossia per quelle entità che occupano meno di 10 persone e che non superano i 2 milioni di euro di fatturato o totale di bilancio annuo, tra i quali rientra, attualmente, un numero significativo di fornitori di crowdfunding.

Per quanto riguarda il primo obbligo, relativo alla gestione dei rischi informatici (punto a), il Consiglio di Amministrazione è incaricato di definire e approvare il Framework e pertanto i suoi membri devono ricevere formazione continua per comprendere i rischi informatici e valutarne l'impatto sulle operazioni.

Il Framework deve includere strategie, politiche, procedure, protocolli e strumenti necessari per proteggere adeguatamente tutti i beni informatici e le risorse TIC, comprese infrastrutture, software, hardware, server, e le aree sensibili come i centri di elaborazione dati. L'obiettivo è garantire che queste risorse siano protette da rischi come danni, accessi non autorizzati o usi impropri.

Obblighi generali	Le microimprese **non sono tenute**:
Strategia di resilienza operativa digitale: definire come attuare il Framework, definendo i rischi informatici e raggiungendo obiettivi specifici nelle TIC.	• All'istituzione di un ruolo che monitori gli accordi conclusi con i fornitori terzi di servizi TIC • Ad attribuire a una funzione di controllo la responsabilità della gestione e della sorveglianza dei rischi informatici • Al riesame annuale del Framework, che è riesaminato periodicamente, nonché in occasione di gravi incidenti TIC o di indicazioni delle autorità di vigilanza • Ad eseguire periodicamente *audit* sul Framework
Identificazione delle funzioni supportate dalle TIC: identificazione, classificazione e documentazione di tutte le funzioni commerciali supportate dalle TIC, dei relativi ruoli e responsabilità, dei patrimoni informativi e delle risorse TIC a supporto delle suddette funzioni, con una revisione annuale del processo.	Ad effettuare una valutazione del rischio in occasione di ogni modifica di rilievo dell'infrastruttura del sistema informatico e di rete, dei processi o delle procedure che incidono sulle funzioni commerciali supportate dalle TIC, sui loro patrimoni informativi o sulle loro risorse TIC Ad effettuare periodicamente, almeno una volta all'anno e in ogni caso prima e dopo la connessione di tecnologie, applicazioni o sistemi, una valutazione del rischio specifica per tutti i sistemi *legacy*
Monitoraggio dei rischi TIC: identificare continuatoivamente i rischi legati alle TIC, inclusi quelli da e verso altre entità finanziarie, e valutare le minacce e vulnerabilità TIC, con un riesame almeno annuale.	
Mappatura dei patrimoni TIC: identificare e mappare le risorse TIC essenziali, comprese quelle remote, di rete e hardware, per identificare quelle considerate essenziali, insieme alla mappatura dei collegamenti e delle interdipendenze tra i diversi patrimoni informativi e risorse TIC	
Gestione dei fornitori terzi: identificare i processi dipendenti da fornitori di servizi TIC e le interconnessioni con i fornitori di servizi essenziali	
Politiche di sicurezza TIC: adottare politiche per garantire resilienza, continuità e sicurezza dei sistemi TIC, mantenendo elevati standard di disponibilità, integrità e riservatezza.	Nessuna esenzione
Rilevazione di attività anomale: implementare sistemi per rilevare tempestivamente anomalie e vulnerabilità TIC, eseguendo test su base regolare.	Nessuna esenzione
Piano di continuità operativa TIC: implementare una politica di continuità operativa specifica per le TIC, integrata con la politica generale di continuità operativa dell'entità finanziaria.	• A sottoporre a *audit* interno indipendente i piani di risposta e ripristino relativi alle TIC; • A inserire nei piani di continuità operativa test sugli scenari di attacchi informatici e del passaggio tra le infrastrutture delle TIC primarie e la capacità ridondante, i backup e le attrezzature ridondanti • A dotarsi di una funzione di gestione delle crisi • A comunicare annualmente alle autorità competenti una stima aggregata dei costi e delle perdite causati da incidenti gravi connessi alle TIC
Backup dei dati: adottare politiche per determinare i dati da sottoporre a backup e la loro frequenza, in base alla criticità delle informazioni o al livello di riservatezza dei dati e le procedure e i metodi di ripristino e recupero.	A mantenere capacità di TIC ridondanti dovendo esclusivamente valutare la necessità di mantenere tali presidi, sulla base del loro profilo di rischio
Comunicazione in caso di crisi: prevedere piani di comunicazione per informare responsabilmente su incidenti TIC rilevanti, che determino responsabilità verso clienti, controparti e pubblico.	Nessuna esenzione
Comunicazione interna ed esterna: stabilire politiche di comunicazione per il personale e gli stakeholder, identificando almeno una persona che sia responsabile della comunicazione sugli incidenti TIC.	Nessuna esenzione
Gestione degli incidenti TIC: implementare procedure per identificare, gestire e notificare gli incidenti TIC, anche nei servizi di pagamento.	Nessuna esenzione
Test di resilienza e sicurezza: predisporre test di resilienza digitale, sui sistemi TIC, e test di penetrazione per verificare la sicurezza.	A predisporre e mantenere un programma di test di resilienza operativa digitale
Gestione dei rischi informatici da terzi: adottare principi per gestire correttamente i rischi TIC derivanti da fornitori esterni.	Ad adottare e riesaminare periodicamente la strategia per i rischi informatici derivanti da terzi

Contatti

Umberto Piattelli
umberto.piattelli@lcalex.it

Sofia Caruso
sofia.caruso@lcalex.it

Gaia Rulli
gaia.rulli@lcalex.it