DORA · SEGNALAZIONE DEGLI INCIDENTI E RESILIENZA

DORA: segnalare gli incidenti. Gestire la resilienza.

Guida pratica per gli enti finanziari: verificare l’ambito, collegare le aree di lavoro e preparare la segnalazione degli incidenti gravi connessi alle TIC.

DORA si applica dal 17 gennaio 2025, ma non a qualsiasi impresa.

Verificate la singola entità giuridica rispetto all’articolo 2, comprese esclusioni e prescrizioni semplificate. Un contratto con un cliente non trasforma automaticamente un fornitore TIC in un ente finanziario soggetto a DORA; possono sorgere obblighi contrattuali e obblighi nel quadro di sorveglianza dei fornitori critici di servizi TIC.

Cinque aree di lavoro collegate

Gestione del rischio TIC
Organizzare responsabilità, inventari, protezione, rilevamento, risposta e ripristino.

Incidenti
Registrare, classificare ed escalare internamente gli incidenti; segnalare i casi gravi.

Test di resilienza
Mantenere un programma proporzionato che includa funzioni critiche e dipendenze.

Terze parti TIC
Gestire registri, contratti, rischi di concentrazione, monitoraggio e opzioni di uscita.

Apprendimento e condivisione
Usare gli insegnamenti degli incidenti; le informazioni sulle minacce informatiche possono essere condivise.

Tempi di segnalazione per un incidente TIC grave

4 h / 24 h
Notifica iniziale
Il prima possibile; entro 4 h dalla classificazione come grave e non oltre 24 h dalla conoscenza.

72 h
Relazione intermedia
Entro 72 h dalla notifica iniziale, anche se lo stato non è cambiato.

1 mese
Relazione finale
Entro un mese dalla relazione intermedia o dal suo ultimo aggiornamento.

Se l’incidente viene classificato come grave oltre 24 ore dopo che l’ente ne è venuto a conoscenza, la notifica iniziale va presentata entro 4 ore da tale classificazione. Inviare gli aggiornamenti richiesti senza indebito ritardo e verificare procedura dell’autorità competente ed eccezioni applicabili.

Valutare la gravità con criteri definiti

Applicate i criteri e le soglie del regolamento (UE) 2024/1772: impatto sui servizi critici, durata, clienti o transazioni, diffusione geografica, perdita di dati e impatto economico. Registrate classificazione, motivazione e orario.

DAL REGOLAMENTO A UNA RISPOSTA CHIARA AGLI INCIDENTI

Sei passi per prepararsi a un incidente

Un processo esercitato riduce le ricerche e i passaggi di coordinamento quando più team e fornitori TIC devono stabilire rapidamente fatti affidabili.

01 · Responsabilità

Nominare per ogni entità giuridica un responsabile dell'incidente, un sostituto, un referente della direzione e un responsabile della segnalazione.

02 · Classificazione

Valutare servizi critici interessati, durata, clienti, transazioni, paesi, perdita di dati e impatto economico secondo le soglie applicabili.

03 · Cronologia

Registrare scoperta, conoscenza, decisioni di classificazione e ogni invio con il relativo fuso orario.

04 · Raccolta dei fatti

Documentare funzioni e impatti, cause note, contenimento, fornitori e stime di ripristino.

05 · Relazioni successive

Preparare la relazione a 72 ore e gli aggiornamenti. Distinguere chiaramente stime e informazioni ancora da verificare.

06 · Chiusura e apprendimento

Completare analisi della causa, impatti effettivi e misure correttive; riportare gli insegnamenti nei test e nella gestione dei fornitori.

Informazioni da avere pronte per la prima segnalazione

ID incidente e orari · funzione critica o importante interessata · motivazione iniziale della classificazione · paesi, clienti o transazioni coinvolti · interruzione e impatto sui dati · misure immediate · fornitori TIC principali · contatto e orario del prossimo aggiornamento. Usare i moduli e il canale richiesti dall'autorità competente.

Due distinzioni importanti

Registrate e classificate gli incidenti relativi alle TIC secondo i criteri DORA; agli organi di vigilanza vanno segnalati gli incidenti gravi. Una minaccia informatica significativa può essere segnalata volontariamente ai sensi dell'articolo 19. Verificate separatamente gli obblighi su dati personali, contratti e altri settori.

Fonti ufficiali · stato giuridico al 8 ottobre 2026

DORA, regolamento (UE) 2022/2554 (in particolare artt. 2, 5-19, 28-30, 64) · regolamento delegato (UE) 2024/1772 (criteri di classificazione) · regolamento delegato (UE) 2025/301 (termini) · regolamento di esecuzione (UE) 2025/302 (moduli) · EIOPA, quadro DORA.

Testi ufficiali: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Limiti

Strumento informativo generale, non consulenza legale, indagine tecnica, valutazione di conformità o segnalazione a un'autorità. Verificare ambito, classificazione, autorità competente, canale e deroghe per la specifica entità giuridica.