DORA · NOTIFICACIÓN DE INCIDENTES Y RESILIENCIA

DORA: notificar incidentes. Gestionar la resiliencia.

Guía práctica para entidades financieras: confirmar el ámbito, conectar las áreas de trabajo y preparar la notificación de incidentes graves relacionados con las TIC.

DORA se aplica desde el 17 de enero de 2025, pero no a todas las empresas.

Compruebe cada persona jurídica conforme al artículo 2, incluidas las exclusiones y los requisitos simplificados. Un contrato con un cliente no convierte automáticamente a un proveedor TIC en entidad financiera sujeta a DORA; pueden surgir obligaciones contractuales y obligaciones dentro del marco de supervisión de proveedores terceros críticos de TIC.

Cinco áreas de trabajo conectadas

Gestión del riesgo TIC
Organizar responsabilidades, inventarios, protección, detección, respuesta y recuperación.

Incidentes
Registrar, clasificar y escalar internamente los incidentes; notificar los casos graves.

Pruebas de resiliencia
Mantener un programa proporcionado que incluya funciones críticas y dependencias.

Terceros TIC
Gestionar registros, contratos, riesgos de concentración, supervisión y opciones de salida.

Aprendizaje e intercambio
Aplicar lecciones de incidentes; puede compartirse información sobre ciberamenazas.

Plazos de notificación de un incidente grave relacionado con las TIC

4 h / 24 h
Notificación inicial
Lo antes posible; en 4 h desde la clasificación como grave y, como máximo, 24 h desde que se tuvo conocimiento.

72 h
Informe intermedio
Como máximo 72 h después de la notificación inicial, aunque no haya cambiado el estado.

1 mes
Informe final
Como máximo un mes después del informe intermedio o de su última actualización.

Si el incidente se clasifica como grave más de 24 horas después de que la entidad tuviera conocimiento, la notificación inicial debe presentarse en las 4 horas siguientes a esa clasificación. Envíe las actualizaciones requeridas sin demora indebida y compruebe el procedimiento de la autoridad competente y las excepciones aplicables.

Valore la gravedad con criterios definidos

Aplique los criterios y umbrales del Reglamento (UE) 2024/1772: impacto en servicios críticos, duración, clientes o transacciones, alcance geográfico, pérdida de datos e impacto económico. Registre la clasificación, su motivo y la hora.

DE LA NORMA A UNA RESPUESTA CLARA ANTE INCIDENTES

Seis pasos para prepararse

Un proceso ensayado reduce las búsquedas y coordinaciones cuando varios equipos y proveedores TIC necesitan confirmar rápidamente los hechos.

01 · Responsabilidad

Designe por persona jurídica un responsable del incidente, suplente, contacto de dirección y responsable de notificación.

02 · Clasificación

Evalúe servicios críticos afectados, duración, clientes, transacciones, países, pérdida de datos e impacto económico frente a los umbrales aplicables.

03 · Cronología

Registre detección, conocimiento, decisiones de clasificación y cada envío con su zona horaria.

04 · Recopilar hechos

Documente funciones e impactos, causas conocidas, contención, proveedores y previsiones de recuperación.

05 · Informes posteriores

Prepare el informe de 72 horas y las actualizaciones. Identifique claramente estimaciones y datos pendientes de verificar.

06 · Cierre y aprendizaje

Complete el análisis de causa, impactos reales y medidas correctivas; incorpore las lecciones a pruebas y gestión de proveedores.

Datos que conviene tener listos para el primer informe

ID del incidente y marcas de tiempo · función crítica o importante afectada · motivo inicial de la clasificación · países, clientes o transacciones afectados · interrupción e impacto en datos · medidas inmediatas · proveedores TIC clave · contacto y hora de la próxima actualización. Use los formatos y el canal exigidos por la autoridad competente.

Dos distinciones importantes

Registre y clasifique los incidentes TIC conforme a los criterios DORA; los incidentes TIC graves deben notificarse a la autoridad. Una ciberamenaza significativa puede notificarse voluntariamente con arreglo al artículo 19. Compruebe por separado las obligaciones sobre datos personales, contratos y otros sectores.

Fuentes oficiales · estado jurídico a 8 de octubre de 2026

DORA, Reglamento (UE) 2022/2554 (en particular arts. 2, 5-19, 28-30 y 64) · Reglamento Delegado (UE) 2024/1772 (criterios de clasificación) · Reglamento Delegado (UE) 2025/301 (plazos) · Reglamento de Ejecución (UE) 2025/302 (formularios) · EIOPA, resumen DORA.

Textos oficiales: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Límites

Material general de trabajo; no es asesoramiento jurídico, investigación técnica, evaluación de conformidad ni notificación a una autoridad. Compruebe ámbito, clasificación, autoridad, canal de notificación y excepciones para la persona jurídica concreta.