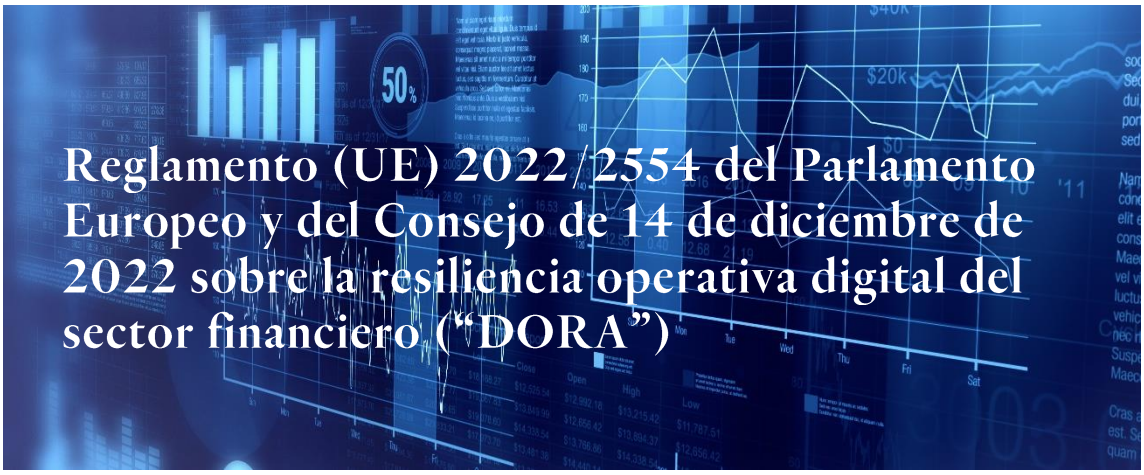
RocaJunyent Informa

Depto. Derecho Protección de Datos, Nuevas Tecnologías y Ciberseguridad
30 de mayo de 2023



El Reglamento DORA actualiza y gestiona los requisitos de riesgo de las tecnologías de la información y la comunicación ("TIC") en todo el sector financiero de la UE de forma homogénea, para que sea capaz de mantener su resiliencia en caso de una interrupción operativa.

¿Cuándo será aplicable?

El Reglamento entró en vigor el 16 de enero de 2023 y será aplicable a partir del 17 de enero de 2025.

¿Cuál es el ámbito de aplicación?

DORA tendrá una aplicación muy amplia y cubrirá las entidades financieras europeas autorizadas (tales como instituciones de crédito, firmas de inversión, entidades de pago, servicios de reporte de datos, intermediadores de seguros, agencias de rating crediticio, etc.), así como a terceros proveedores de servicios TIC (art. 2 DORA).

Esta Alerta tiene un objetivo meramente informativo y no supone asesoramiento jurídico de ningún tipo.

Al mismo tiempo, el Reglamento reconoce que existen diferencias significativas entre las entidades financieras en términos de tamaño, perfiles empresariales o en relación con su exposición al riesgo, y establece un principio de proporcionalidad, de modo tal que impone obligaciones más estrictas a las entidades de mayor tamaño (art. 4 DORA).

¿Qué implica a la organización de la entidad?

La plena responsabilidad del órgano de dirección en la gestión del riesgo TIC de la entidad financiera será un principio general que se traducirá en un conjunto de requisitos específicos, como la asignación de cometidos y responsabilidades claros para todas las funciones relacionadas con las TIC, control, formación en TIC, etc. (art. 5 DORA).

Las entidades deberán disponer de un marco de gobernanza que garantice la gestión efectiva de los riesgos TIC, y designar a un responsable de los sistemas (CISO). Traslada de este modo el enfoque de los sistemas de gestión en seguridad de la información que ya venían definiendo normas como la UNE-ISO 27001 para aquellas empresas que optaban por la certificación.

¿Cómo prevé la gestión de riesgos?

Las entidades financieras deberán contar con un marco de gestión de los riesgos TIC (art.6-16 DORA) completo y sólido, que cubra:

- **Identificación** de las funciones empresariales relacionadas con las TIC y los activos de información;
- **Protección y prevención** diseñando e implementando estrategias, procedimientos, políticas y herramientas de seguridad de las TIC;
- **Detección** de las actividades anómalas relacionadas con las TIC;
- **Respuesta y recuperación,** registrando los incidentes, garantizando la continuidad de la actividad, poniendo en marcha planes de contención y gestión de crisis y poniendo a prueba periódicamente su política de continuidad de negocio y su plan de recuperación;
- **Reducir los tiempos de recuperación,** restaurando los sistemas TIC tras un incidente con un tiempo mínimo de inactividad y una perturbación limitada;
- **Aprendizaje y evolución** (tanto en cuanto a las capacidades y recursos como del personal).

¿En qué consisten las pruebas de resiliencia operativa?

Estas pruebas consisten en comprobar el estado de preparación de los sistemas de las entidades financieras ante incidentes relacionados con las TIC. Las entidades

Esta Alerta tiene un objetivo meramente informativo y no supone asesoramiento jurídico de ningún tipo.

estarán obligadas (art.24-27 DORA) a realizar estas pruebas con los sistemas y aplicaciones TIC esenciales al menos una vez al año. Se contemplan dos tipos de pruebas diferentes según el tamaño e importancia de la entidad, básicas y avanzadas.

¿Habrá que notificar los incidentes?

Las entidades deberán registrar los incidentes y clasificarlos según los criterios de importancia establecidos en DORA (art.17-23 DORA) y solo deberán notificar mediante informe a las autoridades competentes los incidentes relacionados con las TIC que se consideren graves. Las entidades financieras deberán presentar informes iniciales (primer día), intermedios (primera semana) y finales (primer mes) e informar a sus usuarios y clientes cuando el incidente tenga o pueda tener un impacto en sus intereses financieros.

Estas obligaciones de reporte deberán estar coordinadas con otras obligaciones de reporte previstas por otras normas. El reglamento prevé la posibilidad de que los supervisores europeos desarrollen un sistema de estandarización y centralización de los incidentes, a través de la creación de un Hub, si bien los criterios están aún por definir.

¿Qué implica DORA para los proveedores TIC?

Los proveedores TIC (art.28.44 DORA) son compañías que ofrecen servicios digitales y de datos, como servicios en la nube, software y análisis y centros de datos.

DORA parte del principio general de que los riesgos relacionados con los proveedores deben estar integrados en el marco de gestión de riesgos TIC de cada entidad financiera, por lo que éstas tendrán que llevar a cabo una supervisión constante de sus acuerdos con ellos. Además:

- DORA faculta a las autoridades competentes para supervisar a dichos proveedores. Así, se podrán designar proveedores “esenciales”, en función de las entidades financieras que dependan de sus servicios, que serán supervisados por alguna de las autoridades competentes (ABE, AESPJ y AEVM). Éstas podrán solicitar información y realizar investigaciones generales e inspecciones in situ. En caso de incumplimiento, las autoridades pueden imponer multas coercitivas a los proveedores.

- Las empresas que deseen contratar proveedores TIC establecidos en un tercer país y que hayan sido designados como esenciales, solo podrán hacerlo si éstos han establecido una filial en la UE en los últimos 12 meses anteriores a la designación (art.31.12).

Esta Alerta tiene un objetivo meramente informativo y no supone asesoramiento jurídico de ningún tipo.