ECIJA | Calle Serrano, 69. 28006 Madrid
Tel: +34 917 816 160
www.ecija.com

Nota informativa: Reglamento DORA y normativa técnica de desarrollo (RTS)

1 de julio de 2024

El Reglamento (UE) 2022/2554, sobre la resiliencia operativa del sector financiero (en adelante el "***Reglamento***"), es la norma que recoge las medidas de resiliencia digital que han de reunir las entidades financieras y proveedores de servicios TIC que les presten servicios. En el entorno de los riesgos relacionados con el uso, ya extendido, que se da de las tecnologías de la información y la comunicación, y la importancia que presenta el sector para el buen funcionamiento del mercado interior de la Unión Europea, esta herramienta legislativa se antoja crucial. Así, el Reglamento DORA (por sus siglas en inglés "***Digital Operational Resilience Act"***), se adopta con la finalidad de elevar el nivel de armonización y coherencia de los distintos componentes de la resiliencia digital en materia de servicios financieros entre los Estados Miembros, constituyéndose, así, como una *lex specialis* con respecto a la Directiva 2022/2555 (conocida como "*NIS II*").

Por otra parte, el legislador europeo ha considerado la necesidad de desarrollar ciertos preceptos de DORA, a través de su regulación por medio de normativa de carácter más técnico que se promulga a través de actos delegados (por sus siglas en inglés "***Regulatory Technical Standards***" o RTS).

(I) ÁMBITO DE APLICACIÓN

Aunque la norma alude colectivamente a las entidades financieras, esta desglosa su ámbito de aplicación, listando una serie de sujetos obligados entre los que se encuentran **no solo entidades que operan en el sector financiero propiamente dicho, sino también a las entidades que ofrecen servicios de inversión y a aquellas que operan en el sector de los seguros**. Por otra parte, el Reglamento aplica también a sus proveedores terceros de servicios de TIC. Cabe destacar que, si bien es cierto que éstos últimos son también sujetos obligados, la norma les aplicará de forma indirecta, como consecuencia de la relación contractual con las primeras.

(II) NORMAS TÉCNICAS DE DESARROLLO

Como bien se ha indicado, el ecosistema normativo que propone DORA se completa con un conjunto de RTS, de las que ya se encuentran aprobadas y vigentes las siguientes:

- **Reglamento Delegado (UE) 2024/1774:** que desarrolla el conjunto de políticas, procedimientos, protocolos y herramientas que deberán aprobar los órganos de dirección de las entidades para conformar el marco de gestión del riesgo TIC, tanto general, como simplificado. Entre ellas, se encuentran medidas para reforzar, entre otras, el control de accesos, la gestión de claves criptográficas, la gestión de vulnerabilidades y parches y, en general, medidas y controles basados en sistemas de gestión de seguridad de la información.

- **Reglamento Delegado (UE) 2024/1773:** sobre el contenido que ha de reunir la política relativa a los acuerdos contractuales de servicios TIC que sustenten

funciones esenciales o importantes, desarrollando, entre otras, el contenido de las cláusulas que deben recoger dichos acuerdos.

- **Reglamento Delegado (UE) 2024/1772:** acerca del conjunto de criterios que deben seguir las entidades a la hora de clasificar los incidentes TIC y las ciberamenazas importantes, siguiendo un enfoque basado en el riesgo.

- **Reglamento Delegado (UE) 2024/1502:** en el que se desglosan los criterios que han de seguir las Autoridades de Control Europeas para la designación de proveedores TIC esenciales.

A esta primera tanda normativa le seguirá un conjunto de normas que, hoy, siguen su trámite legislativo y se espera sean promulgadas en los próximos meses. Estas versarán sobre las siguientes materias:

- **Normas Técnicas Reglamentarias para la notificación de incidentes graves.**
- **Normas Técnicas Reglamentarias para la subcontratación de servicios TIC que apoyen procesos críticos o esenciales.**
- **Normas Técnicas Reglamentarias sobre la armonización de las condiciones que permiten llevar a cabo las actividades de supervisión.**
- **Normas Técnicas Reglamentarias especificando los elementos relacionados con las pruebas de penetración basadas en amenazas.**

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60