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

Nota informativa: Implicaciones legales del Reglamento DORA frente a las instituciones financieras

Fecha: 20 de octubre de 2023

El objeto de la presente nota es el análisis de los criterios jurídicos impuestos por el Reglamento (UE) 2022/2554 del Parlamento Europeo, "**DORA**", sobre la resiliencia operativa digital en el sector financiero.

(I) Objeto y ámbito de aplicación

El propósito principal de DORA supone el establecimiento de un alto nivel común de resiliencia operativa digital en todas las instituciones financieras de la Unión Europea. Esto significa garantizar que estas instituciones tengan la capacidad de mantener la seguridad de sus redes y sistemas de información, incluso en situaciones de perturbaciones o incidentes de seguridad.

Respecto al ámbito de aplicación, resulta ser extenso e incluye una amplia gama de instituciones financieras, como entidades de crédito, entidades de pago, empresas de dinero electrónico, proveedores de servicios de inversión, gestores de fondos de inversión alternativos, entre otros. Sin embargo, una de las novedades clave es que los **proveedores terceros de servicios de tecnologías de la información y la comunicación** (TIC) también están sujetos a la supervisión del Reglamento DORA. Estos proveedores terceros desempeñan un papel crucial en el ecosistema financiero, por lo que es esencial evaluar y supervisar su capacidad para gestionar los riesgos relacionados con las TIC.

En esta línea, el objetivo perseguido es asegurar que las instituciones financieras sean capaces de **mantener sus servicios financieros y su calidad en todo momento, incluso en caso de incidentes en sus sistemas de TIC**.

(II) Aspectos clave:

El Reglamento DORA establece una serie de requisitos y regulaciones fundamentales para el sector financiero de la UE:

(i) **Gestión de riesgos.** Se impulsa la creación de un marco sólido que asegure un alto nivel de resiliencia operativa digital. En este sentido, las instituciones financieras deben desarrollar un marco sólido para gestionar los riesgos relacionados con las TIC, lo que incluye la protección de activos de información y sistemas de TIC, detección de actividades anómalas y la aplicación de políticas de continuidad de operaciones.

(ii) **Notificación de Incidentes.** Se establecen procedimientos para el registro de incidentes relacionados con las TIC y notificaciones de estos en caso de ser considerados como graves a las autoridades competentes. Estas obligaciones de notificación pueden ser externalizadas a proveedores terceros de servicios.

(iii) **Pruebas de resiliencia operativa.** Para evaluar el nivel de resiliencia operativa digital, las instituciones financieras deben establecer, mantener y revisar un programa de pruebas que aborde todos los riesgos a los que puedan estar expuestas. Además, algunas instituciones, debido a su tamaño y su importancia

sistémica, deben llevar a cabo pruebas avanzadas de penetración basadas en amenazas al menos cada tres años.

(iv) **Regulación de Proveedores Terceros.** Las instituciones financieras deben establecer contratos escritos que detallen los derechos y obligaciones tanto de la entidad financiera como del proveedor tercero de servicios de TIC. Estos contratos son esenciales para garantizar una adecuada gestión de los riesgos derivados de terceros y deben ser complementarios a las regulaciones sectoriales aplicables a la externalización.

(v) **Supervisión continua.** A través del Reglamento DORA, se establece un marco de supervisión para los proveedores terceros esenciales de servicios de TIC en el escenario de prestar servicios a instituciones financieras. Esto implica que estas instituciones deben ser supervisadas de manera similar a como lo serían si los servicios se prestaran internamente.

(III) Conclusiones

En resumen, el Reglamento DORA resulta ser crucial para garantizar la continuidad de los servicios financieros en un entorno cada vez más digitalizado, teniendo por objetivo el fortalecer la resiliencia operativa digital en el sector financiero de la Unión Europea.

Esto se logra a través de una serie de requisitos y regulaciones que abordan la gestión de riesgos, la notificación de incidentes, las pruebas de resiliencia operativa y la supervisión de proveedores terceros de servicios de TIC.

Por último, el Reglamento DORA entró en vigor el 17 de enero de 2023 y será **aplicable de manera directa a partir del 17 de enero de 2025**.

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

Área de Privacidad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60