El Reglamento DORA y sus implicaciones.

Montse Arroyo Sánchez

La digitalización y el riesgo cada vez mayor a sufrir ciberataques ha llevado a la aprobación del Reglamento DORA, el cual, constituye un nuevo marco normativo cuyo objetivo es mejorar la resiliencia operativa y la ciberseguridad en el sector financiero. En este sentido, DORA nace como una lex specialis que establece requisitos uniformes para la seguridad de las redes y sistemas de información de entidades financieras.

El Reglamento (UE) 2022/2554, sobre resiliencia operativa del sector financiero, o más conocido como Reglamento DORA *(Digital Operational Resilience Act)* entró en vigor en enero de 2023, no siendo aplicable hasta 24 meses después, es decir, hasta enero de 2025, dando así un periodo de adaptación de dos años a las entidades afectadas por el mismo.

Este Reglamento constituye un nuevo marco normativo que forma parte de un paquete de medidas sobre finanzas digitales cuyo objetivo es mejorar la resiliencia operativa y la ciberseguridad en el sector financiero.

En definitiva, DORA pretende establecer un marco europeo único para la gestión del riesgo en el ámbito de las tecnologías de la información y la comunicación ("TIC") en el ámbito financiero para mejorar la gestión del mismo a nivel europeo.

Y es que, aunque ya contábamos con normativa en este sentido, la Directiva NIS2, DORA se constituye como una lex specialis porque este reglamento se adopta con la finalidad de elevar el nivel de armonización y coherencia en materia de resiliencia digital en el sector financiero en todos los Estados miembros de la UE.

En cuanto a la aplicabilidad de DORA, el Reglamento se aplicará a las entidades financieras de la Unión Europea, lo cual incluye bancos, empresas de inversión y de créditos, entidades aseguradoras, etc., quedando igualmente bajo el paraguas de vigilancia de DORA los proveedores de servicios TIC de dichas entidades financieras.

El contenido de DORA puede concretarse, a grandes rasgos, en cinco puntos.

En primer lugar, la gestión del riesgo relacionado

con las TIC. Se impulsa la creación de un marco sólido y eficiente que asegure un nivel alto de resiliencia operativa digital. Es fundamental establecer planes y herramientas para proteger, detectar y recuperarse de las interrupciones tecnológicas.

En este sentido, las entidades financieras deberán llevar un seguimiento de la seguridad, deberán disponer de mecanismos de detección rápida de actividades anómalas y aplicarán una política de continuidad, sobre todo, a las actividades esenciales.

... tiene como objetivo mejorar la resiliencia operativa y la ciberseguridad en el sector financiero con el fin de proteger, detectar, contener, recuperar y reparar incidentes relacionados con las TIC.

En segundo lugar, las entidades financieras deberán llevar a cabo un registro de los incidentes relacionados con las TIC o ciberamenazas. Deberán clasificar los incidentes en función de su prioridad y gravedad, y establecer el conjunto de procedimientos y procesos adecuados para mitigar los posibles efectos.

En tercer lugar, las entidades financieras mantendrán un programa de pruebas para evaluar el nivel de resiliencia operativa digital. Este programa debe tener en cuenta todo riesgo específico al que la entidad pueda estar expuesta y cualquier factor que se considere inapropiado.

En cuarto lugar, el Reglamento prevé la posibilidad de que las entidades intercambien información en relación con las ciberamenazas, siempre y cuando dicho intercambio favorezca la resiliencia operativa digital y existan acuerdos que protejan los intercambios, el secreto empresarial, los datos personales y las políticas de competencia.

Por tanto, no podemos perder de vista la necesidad de dar cumplimiento a las disposiciones del Reglamento General de Protección de Datos cuando en dicho intercambio de información se vean comprometidos datos personales.

En quinto lugar, el Reglamento incluye medidas para la gestión del riesgo relacionado con las TIC derivado de terceros que implican que la relación entre la entidad financiera y el tercero esté debidamente recogida en un contrato escrito que contenga los derechos y obligaciones de las partes. De esta forma, el Reglamento recoge aquellas cuestiones a nivel contractual que deben incluir los acuerdos entre las entidades financieras y sus proveedores terceros de servicios TIC. Estas exigencias son mayores cuando afectan a funciones esenciales o importantes.

Ahora bien, el Reglamento de DORA no se queda aquí. El legislador europeo ha considerado necesario desarrollar ciertos preceptos de DORA a través de normativa más técnica que son las normas técnicas de regulación (RTS). A día de hoy, han sido aprobadas y se encuentran vigentes cuatro de estas normas, pero se espera que, a esta primera tanda, le sigan otras cuatro normas técnicas.

Finalmente, en cuanto al régimen sancionador de DORA, las autoridades competentes designadas en cada Estado miembro son las encargadas de supervisar su cumplimiento. En este sentido, estas dispondrán de las facultades de supervisión, investigación y sanción necesarias para velar por el correcto cumplimiento de las obligaciones impuestas por DORA. En nuestro caso, la autoridad competente es el Banco de España.

DORA pretende establecer un marco europeo único para la gestión del riesgo en el ámbito de las tecnologías de la información y la comunicación ("TIC") en el ámbito financiero para mejorar la gestión del mismo a nivel europeo.

En conclusión, como consecuencia del aumento de la digitalización, la falta de un marco regulatorio armonizado para la gestión de riesgos TIC y el incremento de los ciberataques, surge el Reglamento DORA que establece requisitos uniformes para la seguridad de las redes y sistemas de información de las empresas y organizaciones que operen en el sector financiero.

Las entidades financieras deberán clasificar los incidentes en función de su prioridad y gravedad, y establecer el conjunto de procedimientos y procesos adecuados para mitigar los posibles efectos.

Así, el Reglamento DORA crea un marco regulador específico sobre la resiliencia operativa digital conforme al cual las entidades financieras deben asegurarse de que pueden resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC.

...como consecuencia del aumento de la digitalización, la falta de un marco regulatorio armonizado para la gestión de riesgos TIC y el incremento de los ciberataques, surge el Reglamento DORA que establece requisitos uniformes para la seguridad de las redes y sistemas de información de las empresas y organizaciones que operen en el sector financiero.