

NOVEDADES EN LA NORMATIVA RELATIVA A LOS RIESGOS ASOCIADOS A LA TECNOLOGÍA Y A SU SUPERVISIÓN

En un mundo cada vez más digitalizado, las entidades financieras dependen completamente de la tecnología para poder desarrollar sus modelos de negocio y ofrecer a sus clientes los productos y servicios que estos demandan de modo fiable y seguro. Por ello, para garantizar la resiliencia operacional de las instituciones, esto es, su capacidad para continuar prestando servicios ante todo tipo de situaciones adversas, es crucial asegurar la resiliencia de sus sistemas tecnológicos, no solo frente a los cada vez más frecuentes y sofisticados ciberataques de los que son objeto las entidades financieras, sino también frente a otro tipo de situaciones disruptivas, como los desastres naturales o la pandemia global de COVID-19.

En los últimos cinco años, Europa ha realizado un importante esfuerzo regulador encaminado a mejorar la resiliencia del sector financiero, y muy especialmente su resiliencia tecnológica o digital, destacando dos iniciativas:

- i) *Directrices de la Autoridad Bancaria Europea (EBA, por sus siglas en inglés) sobre gestión de los riesgos de TIC y de seguridad (EBA/GL/2019/04).*
- ii) *Propuesta de reglamento de la UE Digital Operational Resilience Act (DORA).*

En primer lugar, las directrices de la EBA, que están en vigor desde el 30 de junio de 2020, son de aplicación a entidades de crédito, entidades de pago y entidades prestadoras del servicio de información sobre cuentas, entidades de dinero electrónico y firmas de inversión, siempre teniendo en cuenta el principio de proporcionalidad. Incluyen también obligaciones para las autoridades competentes.

Entre los aspectos más destacados de estas directrices podemos citar sus requerimientos sobre gobierno y estrategia, gestión de riesgos y pruebas de seguridad y de continuidad de negocio, que armonizan y elevan el nivel de exigencia.

En cuanto a la propuesta legislativa del nuevo reglamento, DORA, el texto se publicó a finales de septiembre de 2020 y está actualmente en fase de discusión en el Consejo Europeo y en el Parlamento Europeo. DORA forma parte de la estrategia de finanzas digitales de la Comisión Europea, y su objetivo es mitigar los riesgos asociados a la digitalización y mejorar la resiliencia del sector financiero europeo.

Por primera vez en la Unión Europea, habrá una regulación única sobre resiliencia tecnológica aplicable a todo tipo de instituciones financieras, de modo proporcional a su tamaño y complejidad. El texto contiene requerimientos para las entidades sobre la gestión de los riesgos asociados a la tecnología, la gestión y notificación de incidentes tecnológicos, la realización de pruebas sobre la resiliencia de los sistemas y la gestión de sus relaciones con terceras partes. También fomenta la compartición de información entre instituciones y la cooperación entre autoridades.

Una de las grandes novedades de DORA es que establece un marco de vigilancia sobre aquellos proveedores tecnológicos que sean críticos para el sector financiero europeo. Dada la creciente dependencia de las instituciones financieras respecto a sus proveedores tecnológicos, esta propuesta es un paso adelante muy significativo para mejorar el nivel de resiliencia del sector financiero europeo en su conjunto.