esade

Center for Corporate Governance

DORA: Nueva frontera regulatoria en materia de ciberseguridad y reto para los consejos de administración de las entidades financieras

AUTOR

Alicia Muñoz Lombardía

Directora de Gobierno, Regulación y Asesoría Jurídica de Banca Comercial y Privada – Santander España

NED Canal de Isabel II y Presidenta de Santander Seguros

Senior Fellow – Centro de Gobierno Corporativo ESADE.

Marzo 2025

Introducción

El informe de riesgos globales 2025 publicado por el Foro Económico Mundial vuelve a destaca la ciberseguridad y otras amenazas digitales entre las principales perturbaciones de un entorno global cada vez más inestable. La digitalización y la interconexión exacerba riesgos de otra naturaleza, incluso sociales y ambientales, provocando que la sociedad sea más vulnerable en su conjunto.

La ciberseguridad y los incidentes derivados de las tecnologías de la información y comunicaciones (TIC o ICT en inglés), por tanto, son algunos de los principales riesgos que afrontan empresas, organismos públicos y Estados, no solo porque la interrupción o afectación a la continuidad del servicio afecta severamente a la operativa y supone cuantiosos costes económicos, sino también por el impacto reputacional y la pérdida de confianza.

Consecuentemente, estamos ante una cuestión a la que prestan atención los consejos de administración que, de manera creciente, vienen incorporando consejeros con conocimientos y experiencia en tecnología.

La transformación digital y la adopción de las nuevas tecnologías como la inteligencia artificial están en la agenda de las entidades como herramientas para desarrollar nuevos productos y servicios con los que generar valor y relaciones cercanas con los clientes así como mejorar la eficiencia y competitividad. La Unión Europea es especialmente sensible al contexto y la seguridad digital está entre sus prioridades y, a tal fin, en los últimos años ha impulsado diversas iniciativas regulatorias, configurando a tal fin un marco jurídico completo en esta materia en continua evolución para adaptarse a los cambios.

Resulta muy ilustrativa la Comunicación de 8 de marzo de 2018 titulada "*Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador*"[1] en la que la Comisión puso de relieve la importancia de garantizar la seguridad tecnológica del sector y su buen funcionamiento, así como la rápida recuperación ante los incidentes y brechas de seguridad para asegurar la continuidad de los servicios TIC y preservar la confianza de consumidores y mercado.

1 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0109

Los reguladores, tras la crisis financiera, pusieron el acento en asegurar la sostenibilidad y resiliencia del sector financiero desde el punto de vista económico, prudencial y de conducta del mercado. Sin embargo, la alta digitalización y conectividad, que son elementos centrales en la prestación de servicios financieros, están cada más en el foco del regulador. La ciberseguridad se ha convertido en una prioridad de la política financiera y los supervisores, más allá del escrutinio del riesgo operacional, están incrementando exponencialmente las actuaciones y revisiones para asegurar que las entidades están preparadas ante amenazas a la seguridad en red.

Estos son los principios que inspiran el Reglamento DORA, norma de plena actualidad, que persigue reforzar la resiliencia digital de las entidades financieras, estableciendo requisitos para definir un marco robusto de gestión de riesgos y extendiendo a los terceros críticos, proveedores de infraestructuras y servicios, determinadas obligaciones.

Conscientes de esta situación y de las potenciales amenazas, los Consejos de Administración no adoptan en materia Cyber un enfoque reactivo o de mero cumplimiento normativo, sino que vienen demostrando una extraordinaria proactividad en la definición del correspondiente marco de regulación interna, controles y supervisión efectiva para asegurar que la entidad pueda identificar los riesgos y prevenirlos y, en caso de materializarse cualquier tipo de interrupción operativa o brecha, ser capaz soportar y recuperarse en el menor tiempo posible.

DORA: Digital Operational Resilience Act

El Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero[2] o Digital Operational Resilience Act, que entró en vigor el 17 de enero de 2025, es una iniciativa europea destinada a reforzar la capacidad de resistencia o resiliencia operativa digital de las entidades financieras. Persigue que, no solo bancos, sino también compañías de seguros, instituciones de inversión colectiva, proveedores de servicios y sistemas de pagos, puedan prevenir, soportar, responder y recuperarse de cualquier interrupción operativa, incidentes cibernéticos y otras perturbaciones tecnológicas graves.

DORA parte de la obligación para la entidad financiera de realizar un análisis de todos los riesgos derivados de las tecnologías de la información y comunicaciones (TIC) para evitar una sobreexposición, exige trasladar obligaciones específicas a los proveedores tecnológicos críticos como plataformas en la nube o servicios de análisis de datos y prevé que las entidades cuenten con un marco de supervisión y monitorización de estos riesgos.

2 https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962

Gobierno y Organización	Gestión de riego TIC	Gestión y notificación de incidencias	Pruebas de resilencia operativa digital	Riesgo de terceros
· Disponer de marcos internos de gobernanza y control que garanticen una gestión eficaz de todos los riesgos de TIC. · Implicar a la Alta Dirección y al Consejo, establecer roles y funciones, diseñar circuitos de aprobación y control así como disponer de una función de control y gestión del riesgo.	· Contar con un proceso de gestión del riesgo de TIC (indentificación activa, protección y prevención, detección, comunicación) sólido y completo. · Garantizar un alto nivel de resiliencia operativa digital que se ajuste a las necesidades tamaño y complejidad de las entidades.	· Identificar, registrar y clasificar los incidentes relacionados con las TIC. · Notificar los incidentes más graves a las autoridades y a los clientes cuando tenga impacto en sus intereses. · Presentar informes, así como comunicar a sus clientes cuando el incidente tenga un impacto en sus intereses financieros.	· Establecer, mantener y revisar un programa de pruebas de resilencia operativa digital sólido y completo como parte del marco de gestión de riegos TIC. · Realizar pruebas apropiadas de todos los sistemas y aplicaciones de TIC, así como pruebas de penetración guiadas por amenazas sobre las funciones esenciales o importantes.	· Gestionar el riesgo de terceros relacionados con las TIC como un elemento integrante del marco de gestión del riesgo de TIC de las entidades financieras. · Establecer los criterios para determinar los proveedores terceros esenciales de servicios TIC, así como el marco de supervisión por parte de las autoridades de la UE.

El consejo de administración de la entidad tiene la responsabilidad última sobre la gestión en materia TIC y, en concreto, debe:

→ Asumir la responsabilidad general de establecer y aprobar la estrategia de resiliencia operativa digital y fijar, debidamente documentado, un marco interno robusto de gobernanza y control para la gestión de los riesgos cibernéticos. Esto incluye determinar el nivel adecuado de apetito de riesgo relacionado con las TIC de la entidad financiera.

→ Aprobar normas internas. El Reglamento Delegado (UE) 2024/1774[3], desarrolla el conjunto de políticas, procedimientos, protocolos y herramientas de gestión, respaldo y recuperación que deberán aprobar los consejos de administración de las entidades y demás órganos de gobierno.

→ Garantizar que, para la relación con proveedores de servicios críticos digitales y de datos (riesgo de terceros) se han formalizado los correspondientes acuerdos que regulen el nivel de servicio (rendimiento, accesibilidad y seguridad) así como el resto de las obligaciones que prevé el Reglamento.

→ Conocer, a nivel individual o agregado, el lanzamiento, progreso, resultado de las pruebas y riesgos de los proyectos relativos a las TIC que tengan un impacto en las funciones esenciales o servicios críticos de la entidad, de manera periódica y tras la ocurrencia de eventos.

→ Impulsar que los sistemas, infraestructuras, protocolos y herramientas tecnológicas estén actualizados y prevenir la obsolescencia.

3 https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80962

- → Asegurar una adecuada asignación de roles y responsabilidades entre las funciones relacionadas con las TIC (por ejemplo, el Chief Operational Resilience Officer-CORO) y promover los mecanismos de escalado y gobernanza adecuados para garantizar una comunicación, cooperación y coordinación efectiva entre dichas funciones.

- → Estar debidamente informado de las medidas de prevención, de las situaciones de crisis y lecciones aprendidas y constituir la última instancia de escalado en caso de perturbaciones graves.

- → Planificar itinerarios formativos a fin de que los consejeros adquieran y mantengan conocimientos y capacidades suficientes para comprender y evaluar el riesgo relacionado con las TIC y sus repercusiones en las operaciones de la entidad financiera.

- → Dotar, en los presupuestos anuales aprobados por el consejo de administración, una partida adecuada y suficiente para atender todos los requerimientos que exige la norma.

Las autoridades de supervisión tienen un papel activo en la evaluación de la resiliencia operativa digital de las entidades. Según el artículo publicado por el Banco Central Europeo el 10 de marzo de 2025 sobre stress testing de ciberresiliencia desde una perspectiva macroprudencial[4] -que ofrece un análisis exhaustivo de cómo los incidentes de ciberseguridad en una o varias instituciones podrían evolucionar hacia una crisis sistémica-, es necesario modificar dicho marco prudencial para incluir aspectos de riesgo cibernético sistémico en los objetivos intermedios, configurar un marco analítico y de indicadores de seguimiento y desarrollar herramientas específicas para analizar escenarios.

Finalmente, y en relación con las sanciones pecuniarias y otras medidas correctoras, el Anteproyecto de Ley de digitalización y modernización del sector financiero[5], prevé el régimen sancionador para los incumplimientos de DORA e incluye una disposición adicional a la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

En esencia, DORA busca aumentar la seguridad y estabilidad del sector financiero europeo frente a los ciberataques, promoviendo buenas prácticas y estableciendo reglas claras para todos los actores involucrados. Está sirviendo, además, de referencia para el desarrollo de otras reglamentaciones que, como la NIS2[6], ambicionan lograr unos estándares uniformes para el gobierno y gestión de los riesgos TIC en toda la Unión Europea, normas que afectan no solo a bancos sino también a categorías de empresas que prestan servicios críticos como energía, transporte, sanidad, alimentación o servicios digitales.

4 https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/html/ecb.mpbu202502_01~-f4914a46c1.en.html
5 Anteproyecto de ley y proyectos de real decreto para la digitalización y modernización del sector financiero
6 BOE.es - DOUE-L-2022-81963 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Tras varios meses trabajando en profundidad en la implantación de DORA, los consejos de administración de las entidades y el equipo directivo están plenamente concienciados sobre la relevancia del Reglamento sobre resiliencia operativa digital. Ahora el foco tiene que estar en la correcta ejecución de la estrategia de resiliencia, desarrollar un cuadro de mando con indicadores de seguimiento por las distintas líneas de defensa, pruebas de evaluación continua, gestión de incidentes y, por supuesto, asegurar que la cultura de ciberseguridad siga permeando en toda la organización y en la sociedad a través de acciones de concienciación, en coordinación con las administraciones.

Solo con vocación de mejora continua se puede ofrecer una respuesta rápida y contundente a las técnicas cada vez más sofisticadas que emplean los ciberdelincuentes.