Publicado el DORA: Reglamento de Resiliencia Operativa Digital

1. Introducción y Antecedentes

La digitalización y las tecnologías de la información y la comunicación (TIC, en adelante) se han convertido en clave para la prestación de servicios financieros, con evidentes ventajas tanto para los usuarios de dichos servicios como para los suminstradores de los mismos. Frente a dichas ventajas, no debe dejarse de lado la vigilancia y supervisión de los riesgos que de un inadecuado uso de las mismas pueda derivarse, tanto para la estabilidad financiera como para la proteccion de los usuarios de servicios financieros.

En este sentido, La Junta Europea de Riesgo Sistémico (JERS, o ESRB por sus siglas en inglés), tras un análisis realizado en 2020 sobre el ciberriesgo sistémico[1], concluyó que existe un elevado nivel de interconexión entre entidades financieras, mercados financieros e infraestructuras de los mercados financieros, y, en particular, las interdependencias de sus sistemas de TIC. Y esto podría traducirse en una vulnerabilidad sistémica que hay que regular y supervisar.

En la misma línea, el Supervisor Bancario Europeo (SSM) ha incluido de nuevo entre sus prioridades supervisoras para los tres próximos años[2] la digitalización y las TIC. Espera que las entidades estén preparadas ante deficiencias en las estrategias de transformación digital y con marcos de resiliencia operativa.

Por otro lado, aunque el sector financiero de la Unión está regulado por un código normativo único y regido por un sistema europeo de supervisión financiera, las normativas que abordan la resiliencia operativa digital y la seguridad de las TIC no están todavía armonizadas, por lo que se debe desarrollar un código normativo único y un sistema de supervisión para que abarque también la resiliencia operativa digital. Es por eso que se deberá reforzar los mandatos de las autoridades competentes para que puedan supervisar la gestión del riesgo relacionado con las TIC en el sector financiero con el objetivo de proteger la integridad y la eficiencia del mercado interior y facilitar su correcto funcionamiento.

Con este motivo, en noviembre de 2021, tras el acuerdo alcanzado por el Consejo sobre los mercados de criptoactivos y la resiliencia operativa digital, se aprobó el **Paquete de Finanzas Digitales**. El objeto de este paquete es apoyar la innovación y la adopción de nuevas tecnologías financieras, proporcionando al mismo tiempo un nivel adecuado de protección de los consumidores y los inversores.

En cuanto a servicios financieros, el Paquete de Finanzas Digitales consta de varias partes:

- La Estrategia de Finanzas Digitales, cuyo objetivo es hacer que los servicios financieros europeos sean más proclives a la digitalización, y se estimule la innovación responsable y la competencia entre los proveedores de servicios financieros de la UE.
- La Estrategia de Pagos Minoristas, donde su principal objetivo es lograr un sistema de pagos minoristas plenamente integrado en la UE, con formas de pago transfronterizo instantáneo. De esta forma se facilitarán los pagos en euros entre la UE y otros territorios y se fomentará la aparición de soluciones de pago paneuropeas y locales.
- Las propuestas legislativas para un marco regulador de la UE en materia de criptoactivos, que impulsará la innovación, preservando al mismo tiempo la estabilidad financiera y protegiendo a los inversores de los riesgos.
- Y**, el Reglamento sobre la resiliencia operativa digital (DORA, por sus siglas en inglés),** cuyo objetivo es tratar de asegurar que el sector financiero en Europa siga funcionando de forma resiliente en caso de graves perturbaciónes operativas:
    - Creando un marco regulador sobre la resiliencia operativa digital conforme al cual todas las empresas deban asegurarse de que pueden resistir y responder a cualquier tipo de

[1] *Systemic cyber risk*, JERS. Febrero, 2020

[2] Prioridades supervisoras 2023-2025, Supervisión Bancaria del BCE

perturbación y amenaza relacionada con las TIC y recuperarse de ellas. Estos requisitos son homogéneos en todos los Estados miembros de la UE.

- Estableciendo requisitos uniformes para la seguridad de las redes y sistemas de información de las empresas y organizaciones que operan en el sector financiero, así como de terceros esenciales que les presten servicios relacionados con las TIC, como plataformas en la nube o servicios de análisis de datos.

2. Reglamento DORA: Objetivos, y requisitos fundamentales

El Reglamento de Resiliencia Operativa Digital (DORA), que se publicó el 27 de diciembre de 2022 en el Diario Oficial de la Unión Europea, **será efectivo a patrir del 16 de enero de 2023 y se deberá aplicar antes del 17 de enero de 2025**.

El Reglamento DORA afecta, entre otras, a las siguientes entidades: a) entidades de crédito; b) entidades de pago; c) proveedores de servicios de información sobre cuentas; d) entidades de dinero electrónico; e) empresas de servicios de inversión; f) proveedores de servicios de criptoactivos autorizados y emisores de fichas referenciadas a activos; g) depositarios centrales de valores; h) entidades de contrapartida central; i) centros de negociación; j) registros de operaciones; k) gestores de fondos de inversión alternativos; l) sociedades de gestión; m) proveedores de servicios de suministro de datos; n) empresas de seguros y de reaseguros; o) intermediarios de seguros, intermediarios de reaseguros e intermediarios de seguros complementarios; p) fondos de pensiones de empleo; q) agencias de calificación crediticia; r) administradores de índices de referencia cruciales; s) proveedores de servicios de financiación participativa; t) registros de titulizaciones y, u) proveedores terceros de servicios de TIC. Sin embargo, es necesario tener en cuenta que se aplicaría el principio de proporcionalidad.

El Reglamento tiene por objeto consolidar y actualizar los requisitos relativos al riesgo relacionado con las TIC. Así pues, este Reglamento trata las incoherencias de algunos de los actos jurídicos anteriores y hace referencia explícita al riesgo relacionado con las TIC a través de normas específicas sobre: las capacidades de gestión de este riesgo, la notificación de incidentes, las pruebas de resiliencia operativa y el seguimiento del riesgo relacionado con las TIC derivado de terceros. Por consiguiente, el Reglamento debe también reconocer que los incidentes relacionados con las TIC y la falta de resiliencia operativa pueden poner en peligro la solidez de las entidades financieras.

En el Reglamento se desarrollan cinco requisitos clave para las entidades financieras:

Requisitos clave para las entidades financieras
Fuente: AFI

1. **Gestión adecuada de riesgos en el ámbito de las tecnologías de la información y la comunicación (TIC).** Para una correcta gestión del riesgo en el ámbito TIC, las entidades financieras deberán disponer de un marco de gestión del riesgo TIC, que incluirá estrategias, políticas, procedimientos, protocolos y herramientas TIC que sean necesarias. Dentro de este marco, las entidades financieras, entre otras cosas, deberán:

    - Incluir métodos y estrategias de resiliencia operativa digital y métodos para hacer frente a los riesgos TIC.
    - Identificar de forma continua los riesgos TIC.
    - Realizar un seguimiento y control de la seguridad y el funcionamiento de los sistemas y herramientas TIC.
    - Diseñar, adquirir y aplicar políticas, procedimientos, protocolos y herramientas de seguridad de las TIC.
    - Desarrollar los mecanismos de detección de actividades anómalas e incidentes relacionados con las TIC.
    - Desarrollar una política global de continuidad de la actividad en materia TIC como parte de la política global de la continuidad de la entidad financiera.
    - Disponer de planes de comunicación de crisis.

2. **Notificación a las autoridades competentes de incidentes graves relacionados con las TIC y, con carácter voluntario, de ciberamenazas importantes.** Las entidades deberán, entre otras cosas:

    - Desarrollar un proceso de gestión de incidentes TIC y establecer indicadores de alerta temprana y procedimientos de respuesta a los incidentes.
    - Clasificar los incidentes TIC y las ciberamenazas y su repercusión.
    - Notificar los incidentes graves relacionados con las TIC y de forma voluntaria las ciberamenazas importantes.

3. **Pruebas de resiliencia operativa digital.** Las entidades deberán:

    - Establecer, mantener y revisar el programa de pruebas de resiliencia operativa digital que forme parte del marco de gestión de riesgos TIC.
    - Las pruebas de resiliencia operativa digital por medio de pruebas de penetración basadas en amenazas deben ser más pertinentes para las entidades financieras que operen en subsectores esenciales de los servicios financieros y que desempeñen un papel sistémico.
    - Disponer de un programa que esté también preparado para pruebas de las herramientas y sistemas TIC.
    - Y, al menos cada tres años, llevar a cabo pruebas avanzadas consistentes de penetración basadas en amenazas de las herramientas, sistemas y procesos TIC.

4. **Intercambio de información e inteligencia en relación con las ciberamenazas y las vulnerabilidades cibernéticas.** Dado que el riesgo relacionado con las TIC es cada vez mayor y más complejo, la eficacia de las medidas de detección y prevención de dicho riesgo depende en gran medida del intercambio de información sobre amenazas y vulnerabilidades entre las entidades financieras. El intercambio de información contribuye a una mayor concienciación sobre las ciberamenazas. Esto mejora, a su vez, la capacidad de las entidades financieras para evitar que las ciberamenazas se conviertan en incidentes reales relacionados con las TIC y les permite contener de forma más eficaz las repercusiones de tales incidentes y recuperarse con más rapidez.

    Las entidades financieras podrán, por tanto, intercambiar entre sí información e inteligencia sobre ciberamenazas, incluidos indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración. Aunque, deberán notificar a las autoridades competentes su participación en los acuerdos de intercambio de información.

5. **Medidas para la buena gestión del riesgo relacionado con las TIC derivado de terceros.** Estas medidas establecen determinados principios clave para orientar la gestión por parte de las entidades financieras del riesgo relacionado con las TIC derivado de terceros, que son de especial importancia cuando las entidades financieras recurren a proveedores terceros de servicios de TIC para sustentar funciones esenciales o importantes. Las entidades financieras:

    - Gestionarán el riesgo relacionado con las TIC derivado de terceros como un elemento integrante del riesgo relacionado con las TIC dentro de su marco de gestión del riesgo relacionado con las TIC. Además, como parte de su marco de gestión del riesgo TIC, mantendrán y actualizarán a nivel de la entidad, y a nivel subconsolidado y consolidado, un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC.
    - Gestionarán el riesgo relacionado con las TIC derivado de terceros con arreglo al principio de proporcionalidad.
    - Las entidades financieras únicamente podrán celebrar acuerdos contractuales con proveedores terceros de servicios de TIC que cumplan estándares adecuados en materia de seguridad de la información.
    - Deberán implementar programas de riesgo de terceros para evitar interrupciones operativas causadas por ataques a la cadena de suministro e infracciones de terceros.
    - En el caso de los servicios de TIC que sustenten funciones esenciales o importantes, las entidades financieras establecerán estrategias de salida.
    - Los proveedores de servicios en la nube (CSP) se verán obligados a cumplir con los requisitos de DORA si se clasifican como “críticos” cuando:
        - El grado de sustituibilidad, es decir, la facilidad de reemplazar en caso de una interrupción operativa (ya sea internamente o en el entorno del proveedor).
        - El número de entidades financieras que dependen del CSP para la continuidad operativa.
    - Las European Supervisory Authorities (EBA, ESMA y EIOPA) supervisarán el cumplimiento de la CSP críticas a través de inspecciones tanto *in situ* (*on site*) como a distancia (*off site)*.

3. Implicaciones para entidades financieras u otros

Esta normativa tendrá, entre otras, las siguientes implicaciones para las entidades afectadas:

- Se les exigirá a las entidades un **marco de gestión del riesgo relacionado con las TIC**, que incluirá al menos las estrategias, las políticas, los procedimientos, y los protocolos y herramientas de TIC que sean necesarios para proteger debida y adecuadamente todos los activos de información y activos de TIC.
- **Aumentará la supervisión de los riesgos TIC no solo en las entidades financieras**, sino también en los **CSP o servicios digitales, es decir, las grandes tecnológicas**. Esto es relevante, puesto que, por primera vez, empresas que no son entidades reguladas por si mismas pasarán a ser inspeccionadas y supervisadas por las autoridades competentes en fucnión de determinadas actividades que desarrollen con entidades financieras. Se avanza con ello en corregir la dicotomía entre regulación de entidades o regulación de actividades.
- **Deberán registrar todos los incidentes relacionados con las TIC y las ciberamenazas importantes**, clasificándolos y determinando su repercusión. Asimismo, deberán notificar los incidentes graves relacionados con las TIC a la autoridad competente pertinente.
- Las entidades financieras que no sean microempresas **establecerán, mantendrán y revisarán, un programa de pruebas de resiliencia operativa digital sólido y completo** que forme parte del marco de gestión del riesgo relacionado con las TIC.
- Asimismo, por primera vez **podrán y deberán intercambiar información e inteligencia** en relación con las ciberamenazas y las vulnerabilidades cibernéticas.