

NTT DATA

DORA

El desafío del sector financiero
para combatir el riesgo digital

FUTURE
AT HEART



¿QUÉ ES DORA?

El sector financiero afronta el reto de la digitalización y, junto a él, el de la seguridad digital. La proliferación de ciberataques a nivel global ha demostrado la necesidad y urgencia de mitigar su impacto y garantizar la resiliencia operativa de un sector especialmente sensible.

Con ese objetivo, el Consejo Europeo ha aprobado el Reglamento de Resiliencia Operativa Digital (DORA, por sus siglas en inglés), una propuesta de normativa europea cuyo foco es regular la forma en que las empresas financieras gestionan el riesgo digital, ya sea propio (en las infraestructuras IT), o de sus proveedores para el almacenamiento y procesamiento de las operaciones bancarias. De ahí que DORA incluya requerimientos para el sector financiero y sus proveedores, armonizando así los diferentes estándares de resiliencia operativa y ciberseguridad, evitando la actual fragmentación de normativas.

En 2023, DORA será una realidad que afectará a los principales actores del sector financiero de la UE (entidades bancarias, de seguros, mercados financieros, fondos de inversión y de pensiones, etc.) y también a sus proveedores de servicios TIC.

Sus principales ámbitos de actuación se basan en las Best Practices europeas e internacionales destinadas a mejorar la resiliencia cibernética y operativa del sector financiero.

DORA tiene como objetivos:

- Mejorar y racionalizar la **gestión de los riesgos de las TIC** por parte de las entidades financieras.
- Establecer **pruebas exhaustivas de resiliencia** sobre los sistemas TIC.
- **Aumentar la concienciación** sobre los riesgos cibernéticos y los incidentes relacionados con las TIC.
- **Facultar a los supervisores** de los riesgos derivados de la dependencia de proveedores terceros de servicios de TIC por parte de las entidades financieras.
- Crear un mecanismo coherente de **notificación de incidentes** que contribuirá a reducir las cargas administrativas para las entidades financieras y reforzará la eficacia de la supervisión.
- Habilitar el **intercambio de información** entre entidades financieras en relación a la información e inteligencia sobre **ciberamenazas**.

¿QUÉ EXIGIRÁ DORA?

DORA incluye exigentes requisitos vinculados con la gestión de riesgos digitales, la clasificación y notificación de incidentes relacionados con las TIC, pruebas de resiliencia operativa digital, acuerdos entre proveedores de servicios TIC y entidades financieras, supervisión para los proveedores de servicios, etc.

Estas son sus principales exigencias:

- Las medidas de prevención y control que DORA exigirá implantar requerirán un importante esfuerzo de las entidades y conllevarán un cambio en su cultura de gestión de riesgos TIC, que tienen que estar impulsados por el **Consejo de Administración**.
- La **gestión del riesgo de terceros** es uno de los pilares fundamentales de DORA y afecta a tanto a las relaciones contractuales como operativas de las entidades con sus proveedores de servicios TIC. La subcontratación es uno de los orígenes de riesgos TIC más importantes, por lo que deberá mejorarse su marco de gestión y control, así como su operativa.
- DORA es un reglamento que necesitará **involucrar y coordinar a múltiples áreas organizativamente dispersas**. Para ello, se deberán articular los mecanismos y establecer los procedimientos adecuados para asegurar su cumplimiento. De este modo, se ven afectadas áreas que dependen del CTO, CISO y CDO, así como áreas transversales como compras y compliance.
- Fuerte necesidad de **formalización de gobernanza, política y procedimientos**. El riesgo TIC deberá estar alineado con aspectos estratégicos y requerirá ser convenientemente formalizado. Para su operación deberá contar con medios humanos y tecnológicos suficientes, así como inversiones aprobadas al más alto nivel.
- El contenido del reglamento va a permitir desarrollar y empoderar **áreas de las entidades que cada vez están teniendo y van a tener una mayor visibilidad**, como la segunda línea de riesgos TIC (CTRO, Chief Technology Risk Officer) y la gestión de Riesgos de terceros.
- Los **marcos de arquitectura empresarial** (por ejemplo, TOGAF) permiten establecer relaciones bidireccionales entre los procesos de negocio y las diferentes capas tecnológicas que los soportan (sistemas, servicios, procesos y activos IT). La gestión del riesgo tecnológico deberá apoyarse en un modelado de arquitectura empresarial para mapear los sistemas de TIC que dan soporte al negocio y de este modo facilitar el cumplimiento de los requisitos de DORA.
- Las **pruebas de resiliencia operativa**, estrechamente relacionadas con la continuidad de negocio, adquieren una importancia preeminente en este reglamento. Se debe establecer un programa de pruebas sólido y completo.



¿CÓMO PREPARARSE PARA DORA?

La entrada en vigor de DORA situará a las entidades financieras ante el reto de adaptar sus sistemas, procesos y capacidades para cumplir con la nueva regulación. En este sentido, NTT DATA, sexto grupo de servicios de consultoría tecnológica en el mundo, ofrece servicios profesionales ligados al ámbito

regulatorio, de riesgos tecnológicos y ciberseguridad y acompaña a compañías de todo el mundo en este reto. Los servicios de consultoría de NTT DATA para ayudar a las empresas del sector financiero a prepararse para el cambio regulatorio que llega con DORA giran en torno a tres grandes bloques:

- 1. Análisis.** Los expertos de NTT DATA son capaces de realizar un diagnóstico individualizado, exhaustivo y preciso de cada caso, evaluando los riesgos derivados del uso de herramientas tecnológicas, ciberataques y grado de resiliencia frente a eventualidades que puedan suponer un riesgo para el cumplimiento normativo. De esta forma, se detectan los aspectos de mejora y se marca el objetivo a conseguir.
- 2. Estrategia.** Una vez establecido el nivel de madurez de cada compañía, el equipo de consultores diseña un plan estratégico que permita conocer el impacto que DORA tiene en los procesos y estructura organizativa de cada empresa, para después marcar una hoja de ruta que ayude a adaptarse a este nuevo reglamento europeo.
- 3. Puesta a punto.** NTT DATA ofrece un servicio de consultoría integral con equipos expertos en negocio y tecnología, lo que implica que acompaña al cliente a lo largo de todo el proceso, desde el diseño a la implantación, asegurándose de que se dan los pasos correctos y necesarios para obtener las máximas garantías y resultados óptimos.

¿POR QUÉ CONTAR CON NTT DATA?

Hacer frente a la adaptación a DORA con la ayuda de un equipo experto supone diversos beneficios:



Contar con un partner experto para asegurar el **cumplimiento del nuevo reglamento**. NTT DATA es el sexto grupo de servicios de consultoría tecnológica en el mundo y lleva **más de 25 años** colaborando con instituciones financieras líderes.



Disponer de un equipo capaz de **diagnosticar de forma objetiva** la situación real del riesgo, así como los ámbitos de mejora.



Trabajar con un **único partner** para dar respuesta a todos los cambios **funcionales, operativos y tecnológicos**.



NTT DATA

EXPERTOS EN EL SECTOR FINANCIERO

En NTT DATA acompañamos al sector financiero y asesoramos a nuestros clientes de manera integral en el cumplimiento de los requerimientos establecidos por DORA.

Nos avala nuestra amplia experiencia durante más de 25 años colaborando con instituciones financieras líderes, que confían en NTT DATA para la transformación digital de su organización.

Adicionalmente, disponemos de experiencia en la prestación de servicios profesionales adaptados a las necesidades de nuestros clientes como:

- **Ciberseguridad**
- **Gestión de riesgos tecnológicos**
- **Gobernanza**
- **Continuidad de negocio**
- **Gestión del riesgo operacional**
- **Reingeniería de procesos**
- **Outsourcing y outsourcing cloud**
- **Arquitectura empresarial**

NTT DATA, parte del Grupo NTT, es una compañía innovadora global de servicios empresariales y de IT. Ayudamos a nuestros clientes en su proceso de transformación a través de consultoría, soluciones industriales, servicios de procesos comerciales, modernización digital y de IT y servicios administrados.

Somos el mejor partner tecnológico en capacidad para llevar a cabo proyectos a largo plazo, en eficiencia y en eficacia.

