Preguntas frecuentes sobre el Reglamento 2022/2554 de resiliencia operativa digital (Reglamento DORA)

Fecha de actualización 10/02/2026

Índice

Introducción

El 27 de diciembre de 2022 se publicó el Reglamento 2022/2554 (DORA – Digital Operational Resilience Act), de aplicación a partir del 17 de enero de 2025. El Reglamento DORA es aplicable a las entidades financieras que ofrecen servicios en la Unión Europea.

Este documento contiene preguntas frecuentes relacionadas con el Reglamento DORA y la implementación de buenas prácticas y estándares de ciberseguridad. Cada entidad deberá conocer los artículos del Reglamento que le son aplicables en función del tamaño (por ejemplo, si es una microempresa) y del tipo de entidad (si es una empresa de servicios de inversión pequeña y no interconectada o una infraestructura de mercado, etc.).

Las preguntas frecuentes se han agrupado en los distintos pilares del Reglamento:

- Definiciones, ámbito y proporcionalidad
- Gestión del riesgo relacionado con las TIC
- Gestión, clasificación y notificación de incidentes relacionados con las TIC
- Pruebas de resiliencia operativa digital
- Gestión del riesgo relacionado con las TIC derivado de terceros

Adicionalmente, se recomienda consultar las preguntas y respuestas relacionadas con el Reglamento DORA publicadas por las Autoridades Europeas de Supervisión en el siguiente enlace: https://www.esma.europa.eu/joint-committee/joint-qas [1] . Esta lista se actualiza periódicamente con nuevas preguntas (hay un campo que indica la fecha de publicación).

Asimismo, es conveniente acceder periódicamente a la sección de ciberseguridad de la CNMV para consultar referencias normativas, procedimientos y otra información de interés:

https://www.cnmv.es/Portal/Ciberseguridad.

Para cualquier consulta relacionada con el Reglamento DORA se puede dirigir al buzón ciberseguridad@cnmv.es

Este documento no tiene carácter normativo. Tiene como finalidad transmitir al sector y, en concreto, a las entidades financieras sujetas al ámbito del Reglamento DORA, ciertas explicaciones en relación con la aplicación de este Reglamento.

[1] Se recomienda aplicar los siguientes filtros: Legal act: “DORA”, Status: “Final”

Definiciones, ámbito y proporcionalidad

1. Definiciones del Reglamento DORA y glosario de términos

Activo de información: un compendio de información, tangible o intangible, que conviene proteger (art. 3.6 del Reglamento DORA).

Activo de TIC: un activo de software o hardware en las redes y sistemas de información utilizados por la entidad financiera (art. 3.7 del Reglamento DORA).

Ciberataque: un incidente malintencionado relacionado con las TIC provocado mediante una tentativa, perpetrada por cualquier agente de riesgo, de destruir, revelar, alterar, desactivar o robar un activo, de obtener acceso no autorizado a ese activo o de hacer uso no autorizado de él (art. 3.14 del Reglamento DORA).

Detección (función de): la función de detección es el desarrollo e implementación de las actividades apropiadas para identificar la ocurrencia de un evento cibernético (ref. el "Cyber Lexicon" del FSB[2]).

Empresa de servicios de inversión pequeña y no interconectada: una empresa de servicios de inversión que cumple las condiciones establecidas en el artículo 12, apartado 1, del Reglamento (UE) 2019/2033 del Parlamento Europeo y del Consejo (art. 3.34 del Reglamento DORA).

Función esencial o importante: una función cuya perturbación afectaría significativamente al rendimiento financiero de una entidad financiera o a la solidez o continuidad de sus servicios y actividades o cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización, o con sus demás obligaciones con arreglo al derecho aplicable en materia de servicios financieros (art. 3.22 del Reglamento DORA).

Incidente relacionado con las TIC: un único suceso o una serie de sucesos interrelacionados no previstos por la entidad financiera que pone en peligro la seguridad de las redes y sistemas de información y tiene repercusiones negativas en la disponibilidad, autenticidad, integridad o confidencialidad de los datos o en los servicios prestados por la entidad financiera (art. 3.8 del Reglamento DORA).

Incidente grave relacionado con las TIC: un incidente relacionado con las TIC con graves repercusiones negativas en las redes y sistemas de información que sustentan funciones esenciales o importantes de la entidad financiera. Las entidades financieras clasificarán un incidente relacionado con las TIC como grave en base a los criterios especificados en el Reglamento Delegado (UE) 2024/1772.

Inventario de activos TIC: un registro completo y actualizado de todos los sistemas, aplicaciones, datos y componentes tecnológicos que son utilizados por una entidad financiera para prestar sus servicios. Esto incluye tanto los activos internos como aquellos proporcionados por proveedores externos y su cadena de contratación que sustente funciones esenciales o importantes, o partes sustanciales de ellas, y abarca hardware, software, redes, bases de datos y cualquier recurso digital que soporte las funciones esenciales de la organización (arts. 8.4-6 del Reglamento DORA, 4.2 y 30 del Reglamento Delegado (UE) 2024/1774 y el Reglamento de Ejecución (UE) 2024/2956).

[2] https://www.fsb.org/uploads/P130423-3.pdf

Microempresa: una entidad financiera distinta de un centro de negociación, una entidad de contrapartida central, un registro de operaciones o un depositario central de valores, que emplea a menos de diez personas y cuyo volumen de negocios anual o balance anual total es igual o inferior a 2 millones EUR (art. 3.60 del Reglamento DORA).

Órgano de dirección/Consejo de Administración: un órgano de dirección tal como se define en el artículo 4, apartado 1, punto 36, de la Directiva 2014/65/UE, el artículo 3, apartado 1, punto 7, de la Directiva 2013/36/UE, el artículo 2, apartado 1, letra s), de la Directiva 2009/65/CE del Parlamento Europeo y del Consejo, el artículo 2, apartado 1, punto 45, del Reglamento (UE) n.º 909/2014, el artículo 3, apartado 1, punto 20, del Reglamento (UE) 2016/1011 y las disposiciones pertinentes del Reglamento relativo a los mercados de criptoactivos, o las personas equivalentes que dirijan efectivamente la entidad o desempeñen funciones clave de conformidad con el Derecho de la Unión o nacional pertinente (art. 3.30 del Reglamento DORA).

Proveedor tercero de servicios de TIC: proveedor de los servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua, incluidos el hardware como servicio y los servicios de hardware que incluyen la prestación de asistencia técnica a través de actualizaciones de software o firmware por parte del proveedor de hardware y excluidos los servicios telefónicos analógicos tradicionales (arts. 3.19 y 3.21 del Reglamento DORA).

Proveedor tercero esencial de servicios de TIC: un proveedor tercero de servicios de TIC designado como esencial de conformidad con el artículo 31 del Reglamento DORA (art. 3.23 del Reglamento DORA)[3].

Proveedor tercero de servicios de TIC que sustenta funciones esenciales o importantes: proveedor que presta una función (o varias) cuya perturbación afectaría significativamente al rendimiento financiero de una entidad financiera o a la solidez o continuidad de sus servicios y actividades o cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización, o con sus demás obligaciones con arreglo al derecho aplicable en materia de servicios financieros (arts. 3.19 y 3.22 del Reglamento DORA). Por lo tanto, se refiere a servicios de TIC que sean necesarios para el desempeño de funciones críticas o importantes. Los riesgos de estos servicios de TIC también deben considerarse para lograr un alto nivel de resiliencia operativa digital en las entidades financieras[4].

Pruebas de penetración basadas en amenazas (o pruebas TLPT): un marco que imita las tácticas, técnicas y procedimientos de agentes de amenazas reales que se considera que presentan una auténtica ciberamenaza, que permite someter a prueba de forma controlada, a medida y en función de la inteligencia, a los sistemas esenciales de la entidad financiera en producción (art. 3.17 del Reglamento DORA).

En términos prácticos consiste en un tipo de pruebas de hacking-ético donde participa un proveedor de inteligencia para asegurar el realismo de la prueba, un 'equipo rojo' (o red team) que realiza la prueba con el conocimiento y control de un equipo reducido de la entidad financiera y bajo el seguimiento de la autoridad supervisora.

[3] Es importante marcar la diferencia entre los proveedores designados como esenciales para la supervisión directa a nivel europeo y los proveedores de servicios de TIC que para una (o varias) entidad financiera sustentan funciones esenciales o importantes.

[4] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/2750-dora006_en

Resiliencia operativa digital (o ciberresiliencia): la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones (art. 3.1 del Reglamento DORA).

Servicio financiero: los servicios financieros pueden incluir un componente de TIC. Si las entidades financieras prestan servicios de TIC a otras entidades financieras en relación con sus servicios financieros, las entidades receptoras deben evaluar si i) dichos servicios constituyen un servicio de TIC bajo DORA y ii) si las entidades financieras que los prestan y los servicios financieros que ofrecen están regulados por el derecho de la Unión o por la legislación nacional de un Estado miembro o de un tercer país. Si ambas evaluaciones son afirmativas, el servicio de TIC en cuestión se considerará predominantemente un **servicio financiero y no se tratará como un servicio de TIC** a efectos del artículo 3.21 del Reglamento DORA.

En caso de que el servicio sea proporcionado por una entidad financiera regulada que preste servicios financieros regulados, pero no esté relacionado o sea independiente de dichos servicios financieros regulados, el servicio **debe considerarse como un servicio de TIC** según el artículo 3.21 del Reglamento DORA.

El mismo razonamiento se aplica a los servicios auxiliares prestados por una entidad, dependiendo de si dichos servicios auxiliares son servicios financieros regulados o un servicio inseparable, indivisible, preparatorio o necesario para la prestación de un servicio financiero regulado, y no se prestan de forma independiente.

Esta aclaración sobre la diferencia entre servicios financieros y servicios de TIC no menoscaba los requisitos que sean aplicables a las entidades financieras en virtud del Reglamento DORA, a excepción de los requisitos relacionados con la gestión de riesgos de terceros en materia de TIC[5].

Servicios de TIC: los servicios digitales y de datos prestados a través de los sistemas TIC a uno o varios usuarios internos o externos de forma continua, incluidos el hardware como servicio y los servicios de hardware que incluyen la prestación de asistencia técnica a través de actualizaciones de software o firmware por parte del proveedor de hardware y excluidos los servicios telefónicos analógicos tradicionales. (art. 3.21 del Reglamento DORA).

TIBER-ES, marco (Threat Intelligence Based Ethical Red-Teaming - España): marco propiedad del Banco de España[6], basado en la adopción del marco europeo TIBER-EU[7], en el que participa juntamente con la CNMV y la DGSFP. Este marco recoge el modo en que las autoridades, las entidades y los proveedores de servicios de ciberseguridad deben trabajar juntos para alcanzar el objetivo de las pruebas de red teaming (ver la sección de pruebas para más información).

[5] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en
[6] https://www.bde.es/wbe/es/entidades-profesionales/supervisadas/normativa-guias-recomendaciones/tiber-es/
[7] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

2. ¿A qué tipo de entidades financieras supervisadas por la CNMV se aplica el Reglamento DORA?

El artículo 2 del Reglamento DORA indica las entidades financieras bajo el alcance del Reglamento DORA. En el caso de las entidades supervisadas por la CNMV incluye los siguientes tipos de entidades financieras:

- **Empresas de servicios de inversión**[8] (art. 2.1.e) del Reglamento DORA): incluyendo las Entidades de asesoramiento financiero (EAF) y las Sociedades y Agencias de Valores (SAV).
- **Proveedores de servicios de criptoactivos** (art. 2.1.f) del Reglamento DORA) autorizados bajo el Reglamento MiCA[9].
- **Infraestructuras de mercados**[10]: depositarios centrales de valores, entidades de contrapartida central y centros de negociación (art. 2.1.g),h) e i) del Reglamento DORA).
- **Sociedades de gestión** y **gestores de fondos de inversión alternativos** (art. 2.1.k) y l) del Reglamento DORA): incluye sociedades gestoras de IIC[11] (SGIIC), sociedades gestoras de inversión de tipo cerrado[12] (SGEIC), las SICAVs y las sociedades de inversión autogestionadas, excluyendo las sociedades gestoras a las que les aplique el artículo 2.3.a) del Reglamento DORA.
- **Proveedores de servicios de suministro de datos** (art. 2.1.m) del Reglamento DORA)[13].
- **Proveedores de servicios de financiación participativa** (art. 2.1.s) del Reglamento DORA)[14], autorizadas bajo el Reglamento 2020/1503/UE relativo a los proveedores europeos de servicios de financiación participativa para empresas.

3. ¿Qué gestoras quedan excluidas del ámbito de aplicación Reglamento DORA y cuáles son las condiciones de dicha exclusión?

De acuerdo con el artículo 2.3.a) del Reglamento DORA, quedan expresamente excluidas de su ámbito de aplicación los gestores de fondos de inversión alternativos (GFIA) contemplados en el artículo 3.2 de la Directiva 2011/61/UE, siempre que gestionen carteras de fondos cuyos activos gestionados, incluidos los adquiridos mediante apalancamiento, no superen los 100 millones de euros en total, o bien no excedan los 500 millones de euros cuando dichas carteras estén compuestas exclusivamente por fondos no apalancados y sin derechos de reembolso ejercitables durante un periodo mínimo de cinco años desde la inversión inicial.

En consecuencia, estas entidades no están obligadas al cumplimiento Reglamento DORA. No obstante, pueden optar por adoptar voluntariamente su marco de gestión de riesgos TIC y resiliencia digital, especialmente si prevén un crecimiento de sus operaciones que pudiera situarlas en el futuro por encima de los umbrales establecidos.

4. ¿Están las Empresas de Asesoramiento Financiero Nacionales (EAFN) sujetas al Reglamento DORA?

[8] https://www.cnmv.es/portal/Consultas/ESI-Nacionales
[9] https://www.cnmv.es/Portal/Consultas/Proveedores-Servicios-Criptoactivos
[10] https://www.cnmv.es/portal/Consultas/Rectoras/ListadosIM
[11] https://www.cnmv.es/Portal/Consultas/ListadoEntidad.aspx?id=2&tipoent=0
[12] https://www.cnmv.es/portal/consultas/listadoentidad?id=4&tipoent=0
[13] https://www.cnmv.es/portal/mifidii_mifir/mifid-proveedores-datos
[14] https://www.cnmv.es/Portal/Consultas/Servicios-Financiacion-Participativa/Listado-Proveedores

No. Las Empresas de Asesoramiento Financiero Nacionales (EAFN) no se encuentran sujetas al Reglamento DORA, dado que no están incluidas entre las entidades contempladas en el artículo 2.1, letras a) a t), del citado Reglamento. En particular, no se les aplica la definición de empresa de servicios de inversión establecida en el artículo 4, apartado 1, punto 1, de la Directiva 2014/65/UE (MiFID II).

Las EAFN no son consideradas empresas de servicios de inversión, y operan bajo un régimen jurídico diferenciado. Esta distinción se recoge expresamente en el artículo 7 del Real Decreto 813/2023, de 8 de noviembre, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión.

En consecuencia, las EAFN quedan excluidas del ámbito de aplicación Reglamento DORA.

5. ¿Existe en España algún sistema o registro oficial que permita consultar las entidades sujetas al ámbito de aplicación del Reglamento DORA, o le corresponde a cada entidad incluida en el artículo 2 del Reglamento determinar proactivamente su obligación de cumplimiento y prepararse en consecuencia?

No. Es responsabilidad de las propias entidades financieras determinar si les aplica el Reglamento DORA y ser proactivas para cumplir con el Reglamento. No deben esperar a que la CNMV u otra autoridad les comunique que les es aplicable el Reglamento DORA.

6. ¿Están las sucursales de una entidad financiera incluidas en el ámbito de aplicación del Reglamento DORA?

Aunque la responsabilidad de que se implementen los requisitos del Reglamento DORA recae en la entidad legal y la autoridad competente encargada de garantizar el cumplimiento del Reglamento DORA es la del país de su empresa matriz, las sucursales también se encuentran obligadas a cumplir con sus disposiciones como parte integrante de la entidad.

Por ejemplo, si un incidente grave relacionado con las TIC se origina en, o afecta a, una sucursal, debe ser considerado en la notificación correspondiente de la entidad legal a su autoridad bajo el Reglamento DORA, incluyendo la parte relativa al impacto geográfico. Asimismo, en el registro de proveedores de servicios de TIC, debe reflejarse la relación de las sucursales y los servicios de TIC que emplea cada una de ellas.

En lo que respecta a las políticas, procedimientos y herramientas del marco de gestión de riesgos, las sucursales deben integrarse en el sistema de protección de la entidad. Esto implica, entre otros aspectos, que los empleados de las sucursales conozcan las políticas de seguridad aplicables, que los sistemas y dispositivos de la sucursal estén protegidos conforme al marco de gestión de riesgos TIC de la entidad matriz y que el personal participe en los planes de formación correspondientes.

7. ¿Cómo se aplica el principio de proporcionalidad en el Reglamento DORA?

Tal y como indica el artículo 4 del Reglamento DORA, las entidades financieras aplicarán las normas establecidas en los capítulos II, III, IV y el capítulo V sección I de conformidad con el principio de proporcionalidad, teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

A algunas entidades financieras, como las empresas de servicios de inversión pequeñas y no interconectadas, de conformidad con el principio de proporcionalidad se les aplica el **marco simplificado de gestión del riesgo relacionado con las TIC** (art. 16 del Reglamento DORA y título III del del Reglamento Delegado (UE) 2024/1774).
De modo similar, las entidades financieras que se consideran **microempresas** o que están sujetas al marco simplificado de gestión del riesgo relacionado con las TIC cuentan con múltiples exenciones en el articulado del Reglamento DORA[15].

Sin embargo, para las entidades financieras más críticas se articulan obligaciones adicionales como la de realizar pruebas de penetración basadas en amenazas o TLPT (art. 26.8 del Reglamento DORA) bajo notificación de la autoridad, o en el caso de las infraestructuras de mercados requisitos sobre planes de recuperación e instalaciones de respaldo (arts. 12.3 y 12.5 del Reglamento DORA), sobre la política de continuidad (arts. 24.2,3 y 4 del Reglamento Delegado (UE) 2024/1774) o sobre el plazo para notificar incidentes (art. 5.5 del Reglamento Delegado (UE) 2025/301).

8. ¿Para una gestora es de aplicación el marco simplificado de gestión del riesgo relacionado con las TIC, aplicando el principio de proporcionalidad?

No. El principio de proporcionalidad no exime de aplicar artículos de obligado cumplimiento. El marco simplificado de gestión del riesgo sólo es aplicable para las entidades financieras especificadas en el artículo 16.1 del Reglamento DORA.

En el Reglamento no se estipula cómo implementar los artículos, permitiendo a la entidad diseñar una gestión de riesgos TIC que mejor se ajuste a su organización.

9. ¿Cómo se aplica el Reglamento DORA a las microempresas, y qué papel juega el principio de proporcionalidad en su cumplimiento?

El Reglamento DORA no exime a las entidades financieras de su cumplimiento basándose únicamente en su tamaño. En el caso de las microempresas, la clave reside en el **principio de proporcionalidad** (art. 4 del Reglamento DORA). Este principio actúa como un mecanismo de ajuste esencial, permitiendo que las medidas operativas de resiliencia digital sean adecuadas y adaptadas al **perfil de riesgo**, **la magnitud operativa y organizativa, así como a la naturaleza, el alcance y la complejidad de los servicios, actividades y operaciones de una entidad.**

En definitiva, el principio de proporcionalidad actúa como un atenuador normativo, liberando a las microempresas de exigencias técnicas y organizativas desproporcionadas, pero sin dejar a un lado la necesidad de que las mismas realicen un análisis fundado de su exposición e implanten un marco de resiliencia digital sólido, documentado y acorde con su realidad operativa.

[15] Considerando 43 del Reglamento DORA: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R2554#rct_43

Desde la CNMV se valora este principio como un eje fundamental de la supervisión, orientado a garantizar que los requerimientos de resiliencia digital sean realistas, efectivos y adaptados a la realidad de cada entidad. A lo largo de este documento, se expondrán requisitos concretos del Reglamento DORA donde se indicará la existencia, por aplicación directa del principio de proporcionalidad, de excepciones o cumplimiento diferenciado para las microempresas.

Gestión del riesgo relacionado con las TIC

1. ¿Cuál es el papel del Consejo de Administración en la gestión del riesgo TIC?

El Consejo de Administración desempeña un papel crítico y decisivo en la gestión del riesgo TIC, ya que **es responsable** último de garantizar que el marco de gestión del riesgo TIC se implemente de manera efectiva y se alinee con la estrategia y objetivos de la entidad financiera. Su participación activa es fundamental para asegurar la resiliencia operativa digital y la protección de funciones esenciales. Además, el Consejo de Administración es responsable de determinar la tolerancia al riesgo de la entidad, por lo tanto, debe ser capaz de conocer los riesgos tecnológicos a los que se enfrenta su entidad, tener el **conocimiento, competencias y experiencia suficientes** sobre el riesgo TIC y la resiliencia digital y **mantener actualizados** esos conocimientos para evaluar los riesgos tecnológicos y tomar decisiones relativas a su gestión (arts. 5.2, 5.4, 13.5, 17.3.e) del Reglamento DORA y 28.2 del Reglamento Delegado (UE) 2024/1774).

2. ¿Por qué es importante la función de control en la gestión de riesgos TIC?

El Reglamento DORA destaca la relevancia de la separación de funciones e independencia entre la función de gestión y control de riesgos, exceptuando a las microempresas (art. 6.4 del Reglamento DORA y 28.4 del Reglamento Delegado (UE) 2024/1774). De esta manera se evitan posibles conflictos de interés.

Esta separación de funciones garantiza que el marco de gestión de riesgos TIC se implemente adecuadamente y se mantenga actualizado con el tiempo (que se actualice la identificación y valoración de riesgos y sus medidas de mitigación, se planifiquen, ejecuten y se haga seguimiento de las pruebas, se siga el ciclo de vida de la gestión de incidentes y la gestión del riesgo de proveedores de servicios de TIC, se reporte a la dirección y comités de seguridad y riesgos, etc.).

3. Si una entidad está certificada en la ISO 27001 (u otra certificación equivalente), ¿cumple con el Reglamento DORA?

La certificación ISO 27001 (u otra certificación equivalente), certifica el cumplimiento de un conjunto de prácticas estándar de ciberseguridad, no adaptadas a las obligaciones del Reglamento DORA, por lo que su certificación no garantiza el cumplimiento con dicho reglamento al usar otro marco de referencia (por ejemplo, no tiene por qué validar si la entidad notifica a la autoridad en tiempo y forma).

Por lo tanto, la CNMV espera que las entidades financieras, independientemente de la certificación que tengan, realicen un análisis GAP para ver el nivel de adecuación con el Reglamento.

4. Si una entidad financiera es pequeña ¿se espera que tenga contratado un responsable de tecnología (CTO), un responsable de seguridad (CISO) y un auditor de TIC?

La entidad financiera, teniendo en cuenta su perfil particular de riesgo TIC no tiene por qué tener contratados y designados estos roles, ni necesariamente contar internamente con todas esas funciones. La entidad deberá designar las funciones y responsabilidades y valorar qué

funciones delega, mediante contrato, en otras empresas bien intragrupo o bien mediante proveedores externos. En cualquier caso, se espera que se **garantice la independencia** y ausencia de conflictos de interés entre las funciones de gestión, control y auditoría interna o un modelo equivalente de gestión y control (art. 6.4 del Reglamento DORA).

A medida que la entidad crezca (en volumen de negocio, número de empleados o complejidad de sus actividades o servicios de TIC) deberá madurar su capacidad de ciberresiliencia dedicando más recursos propios a la gestión y control, para poder realizar una adecuada gestión y seguimiento de sus riesgos TIC.

El **Consejo de Administración** siempre es el responsable último y debe estar informado para poder tomar decisiones sobre la resiliencia de su entidad. Además, se deben designar funciones para hacer el seguimiento de los servicios de TIC contratados a proveedores. El consejo de Administración debe aprobar la **estrategia de externalización TIC**, y entender y controlar los **riesgos de concentración y dependencia** de terceros críticos.

Se espera que la entidad financiera disponga de conocimientos técnicos suficientes para poder realizar el seguimiento de estas funciones delegadas y **tener suficiente autonomía** en la toma de decisiones sobre los riesgos TIC de la entidad.

5. ¿Cómo se integra la gestión de riesgos TIC con la estrategia empresarial?

La gestión de riesgos TIC no debe tratarse como un proceso aislado, sino que debe estar plenamente integrada en la estrategia y gobernanza de la entidad financiera.

La integración se realiza a través de varios mecanismos clave:

- **Alineamiento estratégico**: La estrategia de resiliencia operativa digital en general (art. 5.2.d) de DORA) y las políticas del marco de gestión de riesgos TIC deben reflejar las prioridades del negocio y apoyar la consecución de objetivos estratégicos de manera que la seguridad de los sistemas TIC (disponibilidad, confidencialidad e integridad) esté directamente vinculada al desempeño empresarial (art. 6.8.a) del Reglamento DORA).
- **Participación de la alta dirección**: El Consejo y la dirección ejecutiva deben supervisar la implementación del marco de riesgos TIC, asegurando que los riesgos se identifiquen, evalúen y mitiguen de manera proporcional a la criticidad de las funciones y activos TIC (art. 5.2 del Reglamento DORA).
- **Evaluación de riesgos en decisiones tecnológicas**: Cualquier inversión, desarrollo o cambio en sistemas y aplicaciones debe incorporar una evaluación de riesgos TIC, identificando posibles impactos sobre funciones esenciales y estableciendo controles preventivos adecuados (art. 8.3 del Reglamento DORA).
- **Planificación de la continuidad y resiliencia del negocio**: La estrategia empresarial debe contemplar escenarios de interrupción tecnológica y planes de contingencia alineados con las funciones esenciales de la entidad, garantizando la continuidad del negocio frente a incidentes TIC (art. 11 del Reglamento DORA).
- **Cultura de riesgo integrada**: La entidad debe fomentar que todos los niveles jerárquicos comprendan la importancia de los riesgos TIC y actúen en consecuencia, incorporando la gestión de riesgos en los procesos de negocio y en la toma de decisiones (arts. 5 y 13.6 del Reglamento DORA).

6. ¿Por qué es importante identificar las funciones esenciales o importantes en el Reglamento DORA?

En numerosos artículos del Reglamento DORA, así como en sus Reglamentos Delegados (UE) y Reglamento de Ejecución (UE), se hace referencias a las funciones esenciales e importantes de la entidad, para que las entidades financieras aborden la resiliencia operativa digital de una manera proporcionada.

Las entidades financieras deben documentar y mantener actualizada la lista de funciones esenciales o importantes, evaluando de forma periódica los riesgos TIC asociados a cada una y garantizando que existan planes de continuidad y recuperación específicos para minimizar el impacto de cualquier interrupción. Una correcta documentación de las funciones esenciales o importantes refuerza la resiliencia operativa digital y asegura que las entidades puedan continuar operando incluso ante fallos tecnológicos o incidentes graves.

En términos prácticos, identificar estas funciones permite a las entidades priorizar recursos, controles y planes de contingencia, enfocando la gestión de riesgos TIC en los ámbitos donde se podría comprometer la operativa crítica.

7. ¿Por qué es importante mantener un inventario de activos TIC?

El inventario de activos TIC constituye la base de toda gestión de riesgos tecnológicos dentro de la entidad, asegurando que las decisiones estratégicas, de seguridad y de continuidad operativa estén fundamentadas en información precisa y actualizada.

Mantenerlo de manera estructurada y revisarlo periódicamente es un requisito indispensable para garantizar la resiliencia operativa digital según DORA[16] (art. 8.6 del Reglamento DORA).

La importancia de mantener un inventario de activos TIC radica en varios aspectos clave:

- **Identificación de activos esenciales:** Permite distinguir qué sistemas y recursos soportan las funciones esenciales o importantes de la entidad financiera y cuáles requieren una atención prioritaria en materia de gestión de riesgos TIC.
- **Evaluación de riesgos:** Facilita la evaluación de amenazas y vulnerabilidades específicas asociadas a cada activo, permitiendo planificar controles preventivos, medidas de seguridad y procedimientos de mitigación de forma eficiente.
- **Planificación de continuidad y recuperación:** Ayuda a diseñar planes de continuidad y recuperación TIC (art. 11 del Reglamento DORA), ya que permite conocer qué activos deben restaurarse primero ante un incidente o interrupción.
- **Supervisión y cumplimiento regulatorio:** Ayuda a cumplir con las obligaciones de supervisión y reporte de DORA (art. 8 del Reglamento DORA y 4.2.b) y 30.1 del Reglamento Delegado (UE) 2024/1774), incluyendo la trazabilidad de activos críticos y la documentación de sus riesgos asociados.
- **Gestión de proveedores y dependencias externas:** Permite identificar qué activos dependen de terceros y evaluar su impacto potencial en caso de fallos del proveedor (art. 28 del Reglamento DORA y el Reglamento de Ejecución (UE) 2024/2956).

8. ¿Cómo se realiza la valoración de riesgos TIC?

[16] Ejemplo https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_inventario_de_activos_2020_v1.pdf

La valoración de riesgos TIC es un proceso estructurado y continuo que permite a las entidades financieras reconocer, categorizar y evaluar las amenazas y vulnerabilidades asociadas a sus activos tecnológicos y funciones esenciales. Este proceso es la base para gestionar eficazmente los riesgos y garantizar la resiliencia operativa digital.

La valoración de riesgos TIC se realiza a través de varias etapas:

- **Inventario y clasificación de activos:** Antes de evaluar riesgos, la entidad debe contar con un inventario actualizado de activos TIC (art. 8 del Reglamento DORA), identificando cuáles son esenciales o importantes y qué funciones dependen de ellos.
- **Análisis de amenazas:** Consiste en identificar eventos que puedan afectar a la disponibilidad, integridad o confidencialidad de los sistemas, incluyendo ciberataques, fallos de hardware/software, errores humanos o interrupciones de proveedores externos.
- **Evaluación de vulnerabilidades:** Se analizan debilidades internas de los sistemas, aplicaciones o procesos que podrían ser explotados por amenazas, utilizando herramientas de análisis de vulnerabilidades, pruebas de penetración y revisiones periódicas de seguridad (art. 8 del Reglamento DORA).
- **Determinación del impacto:** Se evalúa cómo cada riesgo podría afectar a la prestación de funciones esenciales, la estabilidad financiera y la confianza de los clientes, considerando tanto el impacto económico como reputacional.
- **Probabilidad de ocurrencia:** Se estima la frecuencia o probabilidad de que el riesgo se materialice, utilizando datos históricos, escenarios de estrés y análisis predictivos.
- **Tratamiento del riesgo TIC** en donde se establecen las **medidas de mitigación**, los **planes de acción** y reporte al Consejo de Administración.
- **Documentación y priorización:** Cada riesgo identificado se documenta de manera formal y se clasifica según la criticidad y la urgencia, facilitando la asignación de recursos y la definición de controles (art. 8 y 9 del Reglamento DORA).

Este proceso debe ser dinámico y revisado periódicamente, integrando lecciones aprendidas de incidentes anteriores y cambios tecnológicos o regulatorios (art. 8 del Reglamento DORA).

9. ¿Qué controles preventivos se esperan según DORA?

Los controles preventivos son medidas diseñadas para minimizar la probabilidad de que se produzcan incidentes TIC y reducir el impacto de posibles interrupciones sobre las funciones esenciales de la entidad financiera. Estos controles forman parte integral del marco de gestión del riesgo TIC y contribuyen a garantizar la resiliencia operativa digital.

Entre los controles preventivos esperados destacan:

- **Segregación de funciones y responsabilidades**: Separar roles críticos dentro de la gestión de sistemas y procesos TIC para reducir riesgos de errores y evitar conflictos de intereses (art. 6.4, 6.6 y 24.4 del Reglamento DORA).
- **Control de acceso y autenticación reforzada**: Implementar políticas de acceso basadas en el principio de menor privilegio, con autenticación multifactorial cuando sea posible para proteger sistemas y datos sensibles (arts. 20 y 21 del Reglamento Delegado (UE) 2024/1774).
- **Cifrado de información**: Asegurar la confidencialidad e integridad de los datos tanto en reposo como en tránsito, protegiendo información crítica frente a accesos no autorizados (arts. 6 y 7 del Reglamento Delegado(UE) 2024/1774).

- **Copias de seguridad periódicas y pruebas de recuperación**: Establecer rutinas de *backup* y procedimientos de pruebas de restauración de sistemas y datos que garanticen la continuidad de los servicios en caso de fallo (art. 11.6 del Reglamento DORA).
- **Pruebas de vulnerabilidades y auditorías periódicas**: Evaluar de manera regular sistemas, aplicaciones y redes para detectar debilidades antes de que puedan ser explotadas (arts. 28.5, 31.3, 34 y 36 del Reglamento Delegado (UE) 2024/1774).
- **Procedimientos de gestión de incidentes y mantenimientos preventivos**: Documentar procedimientos claros de actuación ante incidentes y realizar actualizaciones y parches de sistemas de manera programada (art. 17 del Reglamento DORA y 10 del Reglamento Delegado (UE) 2024/1774).
- **Gestión del riesgo de proveedores de servicios TIC**: Evaluar los riesgos antes de externalizar funciones críticas, realizar un proceso de diligencia debida con los proveedores, incluir elementos obligatorios en las cláusulas, realizar un seguimiento del servicio, tener un plan de salida, evaluar los riesgos del uso de subcontratistas, etc. (artículos 28 al 30 del Reglamento DORA).
- **Concienciación y formación del personal**: Capacitar a empleados en buenas prácticas de ciberseguridad, manejo seguro de sistemas y respuesta a incidentes, fomentando una cultura de prevención.

Por lo tanto, las entidades financieras no solo deben implementar controles reactivos (para cuando ya ha ocurrido un incidente) sino que también deben implementar medidas preventivas adecuadas. Igualmente, en el ámbito del riesgo de proveedores de servicios de TIC, deben monitorizar que sus proveedores también les garanticen medidas preventivas y reactivas adecuadas.

El Reglamento DORA destaca que la aplicación de estos controles debe ser **proporcional** a la criticidad de las funciones y activos TIC de la entidad (arts. 6 y 8), permitiendo priorizar recursos hacia los elementos que podrían tener un mayor impacto sobre la prestación de servicios financieros. La implementación efectiva de controles preventivos no solo protege contra incidentes tecnológicos, sino que también facilita la supervisión, auditoría y cumplimiento regulatorio, reforzando la confianza de clientes y autoridades competentes.

10. ¿Qué mecanismos de detección de actividades anómalas relacionadas con las TIC se recomienda implementar bajo DORA?

Los mecanismos de detección de actividades anómalas TIC (art. 10 del Reglamento DORA y art. 23 del Reglamento Delegado (UE) 2024/1774) son sistemas, herramientas y procesos que permiten a las entidades financieras identificar de forma temprana incidentes, anomalías o vulnerabilidades que puedan afectar la disponibilidad, integridad o confidencialidad de los datos o en los servicios prestados por la entidad financiera. La implementación de estos mecanismos es esencial para garantizar la resiliencia operativa digital y reducir el impacto de posibles incidentes[17].

Entre los mecanismos de detección recomendados se incluyen:

[17] Es una de las funciones principales de marco de ciberseguridad CSF NIST 2.0 (https://www.nist.gov/cyberframework) junto con la gobernanza, la identificación, la protección, la respuesta y la recuperación.

- **Monitorización continua de sistemas**: Supervisión en tiempo real de servidores, redes, aplicaciones y bases de datos para detectar fallos operativos, interrupciones o degradación del rendimiento.
- **Sistemas de detección de intrusiones** (IDS/IPS): Herramientas que identifican accesos no autorizados, intentos de intrusión o comportamientos anómalos que puedan indicar un ciberataque.
- **Análisis de registros y logs**: Revisión sistemática de registros de actividad de sistemas y aplicaciones para detectar patrones inusuales, errores recurrentes o posibles incidentes de seguridad.
- **Alertas y notificaciones automatizadas**: Configuración de alertas que avisen a los responsables de TIC o de seguridad ante eventos críticos, como caídas de sistemas o brechas de seguridad.
- **Pruebas periódicas y auditorías internas**: Evaluaciones programadas que permiten identificar vulnerabilidades y riesgos no detectados en la operación diaria, contribuyendo a mejorar los controles preventivos.
- **Indicadores clave de riesgo**: Métricas que reflejan tendencias o cambios en la exposición a riesgos TIC, facilitando una detección proactiva de riesgos emergentes.

El Reglamento DORA establece que estos mecanismos deben estar integrados en la gestión de riesgos TIC, documentados y revisados regularmente para asegurar su efectividad (arts. 10 y 25 del Reglamento DORA). Su correcta implementación permite a la entidad anticipar problemas antes de que afecten a funciones esenciales, cumplir con los requisitos de reporte a las autoridades competentes y mejorar continuamente la resiliencia y seguridad de los sistemas TIC.

11. ¿Qué indicadores se utilizan para medir el riesgo TIC?

Los indicadores para medir el riesgo TIC son **métricas cuantitativas y cualitativas** que permiten a las entidades financieras evaluar la exposición a riesgos tecnológicos y la efectividad de los controles implementados (art. 6.8.c) del Reglamento DORA y 2.2.c) y 3.b).ii) del Reglamento Delegado (UE) 2024/1774).

Normalmente, se utilizan indicadores clave de rendimiento o KPIs (K*ey Performance Indicators)*, con datos históricos para evaluar objetivos e indicadores clave de riesgos o KRIs (*Key Risk Indicators),* con enfoque predictivo, para identificar y anticipar riesgos potenciales[18].

Entre los principales indicadores que se recomiendan para medir el riesgo TIC se incluyen:

- **Disponibilidad de sistemas críticos**: Porcentaje de tiempo en que los sistemas esenciales para funciones esenciales están operativos y accesibles, lo que refleja la continuidad de los servicios financieros.
- **Número y severidad de incidentes TIC**: Registro de incidentes reportados, clasificados por impacto, duración y criticidad, permitiendo evaluar la frecuencia de interrupciones y la eficacia de los controles preventivos.
- **Tiempo medio de resolución de incidentes** (MTTR): Indicador que refleja la capacidad de la entidad para restaurar rápidamente servicios y sistemas tras un fallo.

[18] Ejemplo, https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/integrating-kris-and-kpis-for-effective-technology-risk-management

- **Cumplimiento de controles implementados**: Medición del grado en que los controles preventivos y de seguridad se aplican correctamente en los sistemas críticos, incluyendo auditorías y revisiones internas.
- **Porcentaje de activos TIC críticos con controles aplicados**: Proporción de activos identificados como críticos que cuentan con medidas de seguridad, resiliencia y monitorización adecuadas.
- **Evaluación de proveedores de servicios de TIC**: Indicadores relacionados con la estabilidad y desempeño de proveedores externos críticos, incluyendo cumplimiento de acuerdos contractuales y capacidad de recuperación ante incidentes.
- **Alertas de seguridad y anomalías detectadas**: Número de alertas generadas por sistemas de monitorización y detección temprana de riesgos, útil para medir la exposición a amenazas emergentes.

Los indicadores deben ser monitorizados de manera continua, documentados y revisados periódicamente para asegurar su relevancia y efectividad. La entidad debe utilizar los resultados obtenidos para priorizar acciones correctivas, actualizar controles y reforzar la resiliencia de sus sistemas, asegurando que las funciones esenciales puedan operar de manera segura y continua, incluso ante interrupciones tecnológicas o ciberataques.

12. ¿Por qué es importante para una entidad financiera realizar un análisis de impacto de negocio (BIA)?

Como parte de la política global de continuidad de la actividad, las entidades financieras deben llevar a cabo un análisis de impacto en el negocio (BIA, por sus siglas en inglés) de sus exposiciones a perturbaciones graves de la actividad. En un BIA se debe evaluar el impacto potencial de las perturbaciones graves de la actividad mediante criterios cuantitativos y cualitativos, utilizando datos internos y externos y análisis de escenarios, según proceda.

El BIA debe tener en cuenta el carácter esencial de las funciones empresariales identificadas y cartografiadas, los procesos de apoyo, las dependencias de terceros y los activos de información, así como sus interdependencias.

Las entidades financieras garantizarán que los activos de TIC y los servicios de TIC se diseñen y utilicen en plena consonancia con el BIA, en particular en lo que se refiere a garantizar adecuadamente la redundancia [19] de todos los componentes esenciales (art. 11.5 del Reglamento DORA, art. 24, 26 y 28.2.d) del Reglamento Delegado (UE) 2024/1774).

En definitiva, un BIA es fundamental para identificar las funciones esenciales de una organización y evaluar las consecuencias de su interrupción. Permite definir objetivos de recuperación (RTO y RPO, acordados con las áreas de negocio) y servir de base para los planes de continuidad, de recuperación y de respuesta.

13. ¿Qué son la política y los planes de continuidad de la actividad en materia de TIC?

La política y los planes de continuidad de la actividad en materia de TIC son documentos estratégicos y operativos que establecen procedimientos, responsabilidades y recursos necesarios para garantizar la continuidad de las funciones esenciales de una entidad financiera

[19] Esto es, que dichos componentes esenciales incluyan elementos de respaldo, bien activos o pasivos (entrando en funcionamiento en caso de fallo del componente activo).

frente a incidentes tecnológicos, fallos operativos o ciberataques. Esta política y planes buscan minimizar la interrupción de servicios esenciales, proteger la integridad de los datos y asegurar la resiliencia operativa digital, permitiendo a la entidad recuperar sus sistemas y operaciones en los plazos más cortos posibles (art. 11 del Reglamento DORA, art. 24 y 39 del Reglamento Delegado (UE) 2024/1774).

Se espera que los planes de continuidad estén basados en un análisis de impacto en el negocio o BIA (art. 11.5 del Reglamento DORA y art. 24 Reglamento Delegado (UE) 2024/1774) y que estén aprobados por el órgano de dirección de la entidad financiera. En este sentido, se espera que cumplan, entre otros, los siguientes criterios (arts. 24, 25, 26 y 39 del Reglamento Delegado (UE) 2024/1774):

- Estarán **documentados** y serán fácilmente accesibles en caso de emergencia o crisis.
- Asignarán **recursos suficientes** para su ejecución.
- Establecerán los **niveles de recuperación previstos y los plazos para la recuperación** y la reanudación de las funciones y las dependencias internas y externas clave, en particular con respecto a los proveedores terceros de servicios de TIC.
- Determinarán las **condiciones que pueden motivar su activación y las medidas que deben adoptarse** para garantizar la disponibilidad, continuidad y recuperación de los activos de TIC de las entidades financieras que sustenten funciones esenciales o importantes.
- Determinarán las **medidas de restauración y recuperación** en relación con las funciones empresariales esenciales o importantes, los procesos de apoyo, fallos en proveedores terceros y los activos de información, así como sus interdependencias, con el fin de evitar efectos adversos en el funcionamiento de las entidades financieras.
- Determinarán **procedimientos y medidas de copia de seguridad** que especifiquen el alcance de los datos objeto de dicha copia y la frecuencia mínima de su realización, de acuerdo con el carácter esencial de la función que utilice los datos de que se trate.
- Contemplarán **diferentes opciones ante la eventualidad de que la recuperación no sea viable a corto plazo** debido a los costes, los riesgos, la logística o circunstancias imprevistas.
- Especificarán los **mecanismos de comunicación interna y externa,** incluidos los planes para el traslado a la instancia jerárquica superior. Deben estar reflejados los **responsables** y/o cadena de mando para la coordinación y activación de los planes de continuidad de la actividad en caso de contingencia.
- Los planes de continuidad de la actividad y los planes de respuesta y recuperación **se someterán a prueba,** al menos anualmente, para evaluar si dichos planes son capaces de garantizar la continuidad de las funciones esenciales o importantes (ver pregunta siguiente).
- En el caso de entidades financieras que no sean microempresas ni entidades a las que les aplique el marco simplificado de gestión de riesgos, estos planes deberán estar sometidos a **auditorías internas independientes** (art. 11.3 del Reglamento DORA).

En el caso de las entidades para las que es de aplicación el marco simplificado de gestión de riesgos TIC, los planes de continuidad deben incluir, al menos, medios de respaldo y restablecimiento de datos (art. 16.1f) del Reglamento DORA).

14. ¿Con qué periodicidad deben probarse los planes de continuidad de la actividad?

El Reglamento DORA establece que los planes de continuidad de la actividad y los planes de respuesta y recuperación en materia de TIC en relación con los sistemas de TIC que sustenten todas las funciones deben ser probados **al menos una vez al año**, así como en caso de que se produzca cualquier cambio sustancial en los sistemas de TIC que sustenten funciones esenciales o importantes. El resultado de dichas pruebas se deberá tener en cuenta en la **revisión de la política de continuidad** (art. 11.6 del Reglamento DORA y art. 25) del Reglamento Delegado (UE) 2024/1774).

En el caso de las **entidades** para las que es de aplicación el **marco simplificado de gestión de riesgos TIC**, de manera similar, deben ser probados al menos una vez al año en el caso de los procedimientos de copia de seguridad y restauración, o cada vez que se produzca un cambio importante en el plan de continuidad de la actividad. (art. 40.1 del Reglamento Delegado (UE) 2024/1774).

15. ¿Qué beneficios aporta un mapa de riesgos al proceso de priorización de los riesgos TIC?

Un mapa de riesgos es una herramienta visual que permite representar gráficamente los riesgos en función de su probabilidad de ocurrencia y el impacto potencial sobre las funciones esenciales o importantes de la entidad. Esta representación facilita una visión global del entorno de riesgo tecnológico que permite a la alta dirección tomar decisiones informadas, focalizar inversiones en seguridad y continuidad, y cumplir con los requerimientos de supervisión y reporte ante las autoridades competentes.

En definitiva, un mapa de riesgo es una herramienta visual y comprensible que mejora la comunicación entre áreas técnicas y directivas, fomentando una cultura de gestión del riesgo.[20]

16. ¿Por qué es importante revisar el marco de gestión de riesgos relacionado con las TIC? ¿Con qué periodicidad debe revisarse?

La continua evolución de las TIC y el panorama cambiante de amenazas hacen imprescindible que las entidades mantengan su marco de gestión de riesgo TIC en constante revisión y actualización. La digitalización, la adopción de nuevos modelos de tecnologías, así como la creciente sofisticación de los ciberataques incrementan la complejidad y exposición de los sistemas, por lo que mantener un marco estático resulta insuficiente para garantizar la resiliencia operativa.

Revisar periódicamente este marco permite incorporar nuevas tipologías de riesgo, adaptar los controles a los cambios tecnológicos y regulatorios, además de fortalecer la capacidad de detección, respuesta y recuperación ante incidentes.

El marco de gestión del riesgo relacionado con las TIC se documentará y **revisará al menos una vez al año, o periódicamente** en el caso de las microempresas y entidades a las que les aplique el marco simplificado de gestión de riesgos, así como cuando se produzcan incidentes graves relacionados con las TIC, y siguiendo las instrucciones de supervisión o conclusiones derivadas de los procesos pertinentes de prueba o auditoría de la resiliencia operativa digital (Considerando (43) y arts. 6.5 y 16.2 del Reglamento DORA).

Los **momentos clave** para revisar el marco incluyen:

[20] Ejemplo: https://www.ismsforum.es/ficheros/descargas/mapaciberriesgosagersisms20191573036836.pdf

- **Tras incidentes significativos:** Cualquier fallo operativo o ciberataque que afecte funciones esenciales debe generar un análisis de causas y la actualización de controles y procedimientos.
- **Cambios tecnológicos o de negocio:** La adopción de nuevas aplicaciones, sistemas o infraestructuras, así como modificaciones en los servicios prestados, requieren revisar los riesgos asociados y adaptar el marco.
- **Actualizaciones regulatorias:** Los cambios en el Reglamento DORA o en otras normativas relacionadas con la gestión de riesgos TIC deben integrarse en los procedimientos, controles y políticas internas.
- **Evaluaciones internas y auditorías:** Las revisiones periódicas, auditorías internas y ejercicios de pruebas de continuidad deben servir para ajustar y mejorar continuamente el marco.
- En caso de que **la autoridad competente que lo solicite se presentará un informe sobre la revisión del marco de gestión del riesgo** relacionado con las TIC (art. 6.5 del Reglamento DORA). En el capítulo V del Reglamento Delegado (UE) 2024/1774 se pueden encontrar las especificaciones para la realización de dicho informe.

En definitiva, el proceso de revisión implica documentar las actualizaciones, comunicar los cambios a la alta dirección y al personal implicado, y ajustar los planes de continuidad, controles preventivos y mecanismos de monitorización según corresponda. De este modo, la entidad asegura que su gestión del riesgo TIC sea proactiva, dinámica y resiliente, manteniendo la protección de funciones esenciales y el cumplimiento de las obligaciones regulatorias.

17. ¿Qué buenas prácticas pueden reforzar la gestión del riesgo relacionado con las TIC?

Las buenas prácticas para la gestión de riesgos TIC, conforme al enfoque del Reglamento DORA, se orientan a establecer un marco sólido, continuo y alineado con la estrategia de la entidad. Entre las más destacadas se encuentran:

- **Gobernanza y responsabilidad clara:** Asegurar que la alta dirección asuma la responsabilidad última sobre la gestión del riesgo TIC (art. 5 del Reglamento DORA), integrándola en la estrategia corporativa y en la toma de decisiones y se asignen roles y responsabilidades. Definición clara del **apetito de riesgo TIC**, con métricas comprensibles.
- **Establecimiento de un marco de control, gestión y auditoría interna:** Garantizar un nivel adecuado de independencia para evitar conflictos de interés. Se garantizará la separación e independencia de las funciones (art. 6.4 del Reglamento DORA).
- **Gestión continua de riesgos TIC**: Mantener un proceso sistemático para identificar, analizar y evaluar los riesgos derivados del uso de TIC, incluyendo los tecnológicos, de ciberseguridad, de terceros y de continuidad operativa. con un enfoque basado en funciones críticas (no en sistemas)
- **Mapa y priorización de riesgos**: Representar los riesgos mediante un mapa de riesgos TIC, actualizándolo periódicamente para reflejar la evolución tecnológica y las nuevas amenazas, priorizando según impacto y probabilidad.
- I**ntegración con otros marcos de control:** Coordinar la gestión del riesgo TIC con los marcos de riesgo operacional, continuidad de negocio y ciberseguridad, garantizando coherencia y visión global.
- **Medidas preventivas y controles efectivos**: Implementar controles técnicos, organizativos y procedimentales proporcionales al nivel de riesgo identificado, incluyendo políticas de seguridad, gestión de accesos y protección de datos.

- **Monitorización y detección temprana**: Establecer mecanismos de seguimiento continuo para detectar anomalías, vulnerabilidades e incidentes, apoyándose en indicadores clave de riesgo (KRIs) y de rendimiento (KPIs) y alertas tempranas.
- **Planes de respuesta y recuperación**: Diseñar e integrar planes de contingencia y recuperación ante incidentes TIC, probándolos regularmente para garantizar su efectividad (art. 11 del Reglamento DORA).
- **Formación y concienciación**: Promover una cultura de ciberresiliencia, formando al personal en la identificación de riesgos, respuesta ante incidentes y buenas prácticas de seguridad.
- **Revisión y mejora continua del marco**: Evaluar periódicamente la eficacia del marco de gestión de riesgos, incorporando lecciones aprendidas, resultados de auditorías y cambios regulatorios o tecnológicos.

Gestión, clasificación y notificación de incidentes relacionados con las TIC

1. ¿Qué se considera un "incidente relacionado con las TIC" según el Reglamento DORA?

Un incidente relacionado con las TIC es cualquier suceso o serie de sucesos interrelacionados no previstos por la entidad financiera, que interrumpe o degrada el funcionamiento normal de los sistemas TIC, poniendo en riesgo su capacidad de operar o la seguridad de la información (art. 3.8 del Reglamento DORA).

El incidente ocurre de manera inesperada o fuera del control de la entidad, afectando a los activos tecnológicos utilizados para prestar servicios, impidiendo la correcta prestación de los mismos. Además, un incidente relacionado con las TIC produce un efecto adverso en uno o varios de estos aspectos:

- **Disponibilidad**: los datos solicitados por la entidad financiera, sus clientes o sus contrapartes son inaccesibles o inutilizables de forma temporal o permanente.
- **Autenticidad**: la fiabilidad de la fuente de los datos ha sido puesta en peligro.
- **Integridad**: modificación no autorizada de datos que deriva en datos inexactos o incompletos.
- **Confidencialidad**: acceso no autorizado a datos o divulgación de información sensible.

Es importante tener en cuenta que este concepto abarca:

- incidentes técnicos; caídas de sistemas, fallos de red, errores de software, interrupciones en servicios críticos, corrupción de datos, etc.; e
- incidentes de ciberseguridad: ataques distribuidos de denegación de servicio (DDoS), infecciones por software malicioso (incluyendo el ransomware), accesos mediante robo de credenciales o filtraciones de información, entre otros.

2. ¿Qué elementos debe incluir el proceso de gestión de incidentes?

Las entidades financieras deben disponer de un proceso sólido y documentado para la gestión de incidentes relacionados con las TIC, que abarque desde su detección hasta su cierre y revisión posterior (art.17 del Reglamento DORA).

Los elementos esenciales del proceso de gestión de incidentes son:

- **Detección y registro inmediato de incidentes**: la entidad debe contar con mecanismos de monitorización continua que permitan identificar de forma temprana los incidentes o anomalías TIC (art. 10 del Reglamento DORA). Todos los incidentes, independientemente de su gravedad, deben registrarse en un inventario interno con información suficiente para su análisis posterior (art. 17.3.b) del Reglamento DORA).
- **Clasificación y evaluación de gravedad**: una vez detectado, el incidente debe ser categorizado en función de su gravedad. El Reglamento Delegado (UE) 2024/1772 establece, en el Capítulo 1, una serie de criterios de clasificación destinados a homogeneizar el proceso de evaluación. Esta clasificación determinará si el incidente debe notificarse a la autoridad competente y si deben aplicarse otros planes de actuación y escalado, como la activación del plan de continuidad (art. 11.2.c) y 17.3.f) del Reglamento DORA).
- **Funciones, responsabilidades y comunicación**: se deben asignar las funciones y responsabilidades que deben activarse según el escenario. El proceso también debe

establecer líneas claras de comunicación tanto interna como externa y mecanismos de escalado rápido hacia la alta dirección, responsables de TIC y de continuidad de negocio. Debe garantizarse que, al menos, los incidentes graves relacionados con las TIC se pongan en conocimiento de los altos directivos pertinentes y que se informe de ellos al órgano de dirección, explicando sus repercusiones, las medidas adoptadas como respuesta y los controles adicionales que se prevé implantar como resultado de estos incidentes graves relacionados con las TIC (art. 5.2.i), 14 y 17.3 del Reglamento DORA).

- **Contención, mitigación y recuperación:** se deben definir procedimientos operativos y técnicos para aislar el incidente, limitar su propagación, recuperar la operativa normal y restaurar la integridad de los datos o servicios afectados. Estos procedimientos deben estar coordinados con los planes de continuidad y recuperación previstos en el artículo 11 del Reglamento DORA.
- **Notificación a las autoridades competentes** según proceda (art. 19 del Reglamento DORA).
- **Documentación y trazabilidad**: todo el ciclo del incidente debe documentarse: detección, análisis, decisiones, medidas adoptadas, comunicaciones internas y externas, y resultados. Esta documentación sirve de base para auditorías internas, revisiones supervisoras con la autoridad y, en el caso de un delito, para interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.
- **Análisis posterior y lecciones aprendidas** ("forense"): tras la resolución del incidente, la entidad debe analizar las causas raíz[21] y extraer lecciones para mejorar sus controles, políticas y procedimientos. También debe evaluar si es necesario actualizar el marco de gestión de riesgos TIC o de continuidad operativa (art. 6.5 y 13 del Reglamento DORA).
- **Coordinación con terceros y proveedores de servicios de TIC**: si el incidente afecta a un proveedor externo o intragrupo, el proceso debe prever cómo se gestionan las comunicaciones y responsabilidades conjuntas. En la gestión del riesgo relacionado con las TIC derivados de terceros se exige que los contratos con proveedores de servicios de TIC incluyan obligaciones específicas de notificación y cooperación en caso de incidente (art. 30.2.f) del Reglamento DORA).

Es importante que las entidades estén lo mejor preparadas, en la medida de lo posible, implementando este proceso de gestión, formando a los empleados y roles implicados, haciendo pruebas y simulacros, etc. para que cuando ocurra un incidente se evite la improvisación.

3. ¿Qué criterios determinan el carácter esencial de un servicio afectado por un incidente relacionado con las TIC?

Conforme al artículo 6 del Reglamento Delegado (UE) 2024/1772, y con el objetivo de determinar el carácter esencial de los servicios afectados a los que se refiere el artículo 18, apartado 1, letra e), del Reglamento DORA, las entidades financieras evaluarán si el incidente cumple al menos una de las siguientes condiciones:

- Afecta o ha afectado a servicios de TIC o redes y sistemas de información que sustenten funciones esenciales o importantes de la entidad financiera.

[21] Ver en el anexo II del Reglamento de Ejecución (EU) 2025/302 una taxonomía de clasificación de causas raíz o profundas (campos 4.1 al 4.3)

- Afecta o ha afectado a servicios financieros prestados por ellas que requieran una autorización o un registro o que sean supervisados por las autoridades competentes;
- Constituye o ha constituido un acceso efectivo, malintencionado y no autorizado a las redes y sistemas de información de la entidad financiera.

4. ¿Qué incidentes son considerados graves y por tanto son susceptibles de ser notificados a la autoridad competente?

Un incidente se considerará grave a efectos del artículo 19, apartado 1, del Reglamento DORA cuando haya afectado a los **servicios esenciales** a los que se refiere el artículo 6 del Reglamento Delegado (UE) 2024/1772 (ver pregunta anterior) y se cumpla alguna de las condiciones siguientes:

1. Si las redes y los sistemas de información son objeto de un **acceso efectivo, malintencionado y no autorizado**, cuando dicho acceso pueda dar lugar a pérdidas de datos.

2. Si se cumplen **dos o más de los umbrales** de importancia relativa a que se refiere el artículo 9 del Reglamento Delegado (UE) 2024/1772, apartados 1 a 6, expuestos a continuación:

- Se alcanzará el umbral de importancia relativa para el criterio **«clientes, contrapartes financieras y transacciones»** cuando se cumpla cualquiera de las condiciones siguientes:
  a) cuando el número de **clientes afectados sea superior al 10 %** del conjunto de los clientes que utilizan el servicio afectado.
  b) el número de **clientes afectados** que utilizan el servicio afectado sea superior a **100 000.**
  c) el número de **contrapartes financieras afectadas sea superior al 30 %** del conjunto de las contrapartes financieras que llevan a cabo actividades relacionadas con la prestación del servicio afectado.
  d) el número de **transacciones afectadas sea superior al 10 % del número medio diario** de las transacciones realizadas por la entidad financiera relacionadas con el servicio afectado.
  e) la cantidad de **transacciones afectadas sea superior al 10 % del valor medio diario** de las transacciones realizadas por la entidad financiera relacionadas con el servicio afectado.
  f) se hayan visto **afectados los clientes o las contrapartes financieras que se hayan considerado pertinentes** con arreglo a lo establecidos en el artículo 1.3 del Reglamento Delegado (UE) 2024/1772.

  Cuando no pueda determinarse el número real de clientes o contrapartes financieras afectados o el número o la cantidad reales de las transacciones afectadas, la entidad financiera estimará dicho número o dicha cantidad sobre la base de los datos disponibles de períodos de referencia comparables.

- Se alcanzará el umbral de importancia relativa para el criterio **«repercusión en la reputación»** cuando se cumpla cualquiera de las condiciones establecidas en el artículo 2 del Reglamento Delegado (UE) 2024/1772, letras a) a d):
  a) El incidente se ha **reflejado** en los **medios de comunicación**;
  b) El incidente ha dado lugar a **quejas reiteradas de distintos clientes o contrapartes financieras** sobre servicios de cara al cliente o relaciones comerciales esenciales;

c) La entidad financiera **no podrá cumplir los requisitos reglamentarios**, o es probable que no pueda cumplirlos, como consecuencia del incidente;
d) La entidad financiera **perderá, o es probable que pierda, clientes o contrapartes financieras** como consecuencia del incidente, lo que acarreará consecuencias importantes para sus actividades.

- Se alcanzará el umbral de importancia relativa para el criterio **«duración del incidente y duración de la interrupción del servicio»** cuando se cumpla cualquiera de las condiciones siguientes:
  - Cuando la **duración del incidente sea superior a 24 horas**
  - Cuando la duración de la **interrupción del servicio sea superior a dos horas en el caso de los servicios de TIC que sustenten funciones esenciales o importantes.**
- Se alcanzará el umbral de importancia relativa para el criterio de **«extensión geográfica»** cuando **el incidente tenga consecuencias en dos o más Estados miembros** de conformidad con lo establecido en el artículo 4 del Reglamento Delegado (UE) 2024/1772.
- Se alcanzará el umbral de importancia relativa para el criterio «**pérdidas de datos»** cuando tenga o vaya a tener **efectos negativos** en la consecución de los objetivos empresariales de la entidad financiera o en su capacidad para cumplir los requisitos reglamentarios y se cumpla cualquiera de las condiciones siguientes:
  - Cuando la **incidencia sobre la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos** a los que se refiere el artículo 5 del Reglamento Delegado (UE) 2024/1772, tenga o vaya a tener **efectos negativos en la consecución de los objetivos empresariales** de la entidad financiera o en su **capacidad para cumplir los requisitos reglamentarios.**
  - Cuando **las redes y los sistemas de información sean objeto de un acceso efectivo, malintencionado y no autorizado** no contemplado en el apartado anterior cuando **dicho acceso pueda dar lugar a pérdidas de datos**. **La ocurrencia de este apartado por sí solo deriva en la categorización de un incidente como grave** si además ha afectado a un servicio esencial conforme al artículo 6 del Reglamento Delegado (UE) 2024/1772.
- Se alcanzará el umbral de importancia relativa para el criterio **«consecuencias económicas»** cuando los costes y las pérdidas sufridas por la entidad financiera debido al incidente hayan superado o probablemente puedan **superar los 100.000€.**

Se recomienda la revisión de la aplicación de dichos umbrales en la entidad para tener una mejor preparación y poder valorar de forma eficaz si se cumplen los criterios cuando ocurre un incidente (por ejemplo, número medio de transacciones en un día normal, sucursales o clientes en otras regiones geográficas, obligaciones contractuales de los proveedores de servicios de notificar incidentes en plazo, etc.).

5. ¿Cómo deben tratarse los incidentes recurrentes que de manera individual no son considerados graves?

Los incidentes recurrentes que no se consideren individualmente un incidente grave, sí se considerarán como un incidente grave, conforme al artículo 8.2 del Reglamento Delegado (UE) 2024/1772, cuando **cumplan todas las condiciones siguientes**:

- Los incidentes se han producido al menos **dos veces en un plazo de seis meses**.

- Los incidentes tienen **la misma causa subyacente aparente** (Anexo II del Reglamento de Ejecución (UE) 2025/302).
- Se **cumplen colectivamente los criterios** para ser considerados un incidente grave enumerados en el **artículo 8.1 del Reglamento Delegado (UE) 2024/1772.**

Esta previsión no es de aplicación para las microempresas ni a las entidades financieras que les aplica el marco simplificado de gestión de riesgos TIC. El resto de las entidades deberán evaluar **mensualmente** la existencia de incidentes recurrentes.

6. ¿Ante un ataque de denegación de servicio (DoS o DDoS) se debe clasificar el incidente como incidente grave?

En el Reglamento DORA, un ataque de denegación de servicio (DoS/DDoS) **no es automáticamente un incidente grave**, puesto que no constituye un "acceso efectivo, malintencionado a las redes o sistemas de información de la entidad" (artículo 8.1.a) del Reglamento Delegado (UE) 2024/1772), pero **puede serlo** si afecta a funciones críticas o importantes y se superan los umbrales de al menos dos criterios del Reglamento Delegado (UE) 2024/1772 para clasificarlo como grave (por ejemplo, el umbral de pérdida de datos -por la indisponibilidad- o el número de clientes o transacciones afectados durante el ataque, o la duración del ataque, o las pérdidas económicas durante dicha denegación de servicio, etc).

7. ¿Un caso de phishing se considera un "acceso efectivo, malintencionado a las redes o sistemas de información de la entidad" y por lo tanto se debe clasificar el incidente como incidente grave?

Dependerá de la situación y el contexto del phishing[22].

a) **Phising a clientes**:

- Un **phishing puntual a una cuenta del cliente** no se consideraría un "acceso efectivo, malintencionado a las redes o sistemas de información de la entidad" puesto que sólo se ha accedido al espacio privado del usuario y es **responsabilidad del cliente** la protección de su identidad, aunque la entidad financiera pueda ayudar a los clientes con campañas de concienciación o implementar mecanismos de autenticación fuerte. Sin perjuicio de que la entidad también monitorice actividades de cliente anómalas en sus sistemas (por ejemplo, accesos de clientes desde orígenes poco habituales, accesos de múltiples clientes desde el mismo origen, intentos de robo de contraseñas por fuerza bruta, etc.).
- Si los casos de **phishing ocurren en numerosas cuentas de clientes**. La entidad deberá analizar si se debe a una fuga interna de datos (por ejemplo, debido a un ataque de inyección SQL en su página web, un incidente en un proveedor o un puesto de empleado con un malware). En estos casos, si se ha accedido a los datos de clientes desde los sistemas de la entidad, sí sería un incidente grave.

b) **Phising a empleados**: Un caso más claro de incidente grave es si el phishing le ha sucedido a un empleado. Al tener acceso al correo corporativo y/o otra información confidencial de la empresa (como por ejemplo servicios de documentos en la nube o accesos VPN). Este acceso de empleado puede utilizarse para campañas de phishing a otros empleados o clientes, poniendo en peligro a la entidad financiera. En este caso, la protección de la

[22] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2025_7613

identidad de los empleados sí es responsabilidad directa de la entidad financiera bajo el Reglamento DORA.

8. ¿Cómo reportar a la CNMV un incidente grave relacionado con las TIC?

Las entidades financieras, para cumplir con la obligación de notificación de incidentes graves bajo el Reglamento DORA, deben seguir las indicaciones del procedimiento publicado a tal efecto en la web de la CNMV, sección de ciberseguridad[23].

Se recomienda revisar periódicamente dicha web por si se actualiza algún procedimiento o se publica nueva información de interés.

9. ¿Cuál es el plazo para remitir la notificación inicial a la autoridad competente de un incidente grave conforme a DORA?

Las entidades financieras presentarán la notificación inicial a la que se refiere el artículo 19, apartado 4, letra a) del Reglamento DORA lo antes posible, pero, en cualquier caso, en un plazo de cuatro horas a partir de la clasificación del incidente relacionado con las TIC como grave y **a más tardar veinticuatro horas** después del momento en que la entidad financiera haya tenido conocimiento de dicho incidente (art. 5.1 a) del Reglamento Delegado (UE) 2025/301).

Si dicho plazo tiene lugar en día inhábil, se debe tener en cuenta la Q&A relacionada más adelante.

10. ¿Cuál es el plazo para remitir la notificación intermedia a la autoridad competente de un incidente grave conforme a DORA?

Las entidades financieras presentarán la notificación intermedia a la que se refiere el artículo 19, apartado 4, letra b) del Reglamento DORA **a más tardar en un plazo de setenta y dos horas a partir de la presentación de la notificación inicial**, incluso cuando la situación o la gestión del incidente no haya cambiado con arreglo a este mismo artículo; las entidades financieras presentarán un informe intermedio actualizado sin demora indebida y, en cualquier caso, cuando se hayan recuperado las actividades regulares (art. 5.1 b) del Reglamento Delegado (UE) 2025/301).

Por lo tanto, tras la notificación inicial:

- Si la entidad ha recuperado sus actividades dentro de las primeras 72 horas, solo deberá enviar un informe intermedio.
- Si la entidad no ha recuperado sus actividades en ese plazo, deberá enviar:
    - Un primer informe intermedio antes de que se cumplan las 72 horas,
    - Los informes intermedios adicionales que sean necesarios para actualizar su situación,
    - Otro informe intermedio cuando las actividades hayan sido recuperadas.

[23] https://www.cnmv.es/Portal/Ciberseguridad

Si dicho plazo tiene lugar en día inhábil, se debe tener en cuenta la Q&A relacionada más adelante.

11. ¿Cuál es el plazo para remitir la notificación final a la autoridad competente de un incidente grave conforme a DORA?

Las entidades financieras presentarán la notificación final a la que se refiere el artículo 19, apartado 4, letra c) del Reglamento DORA, a más tardar **un mes después de la presentación del último informe intermedio** notificado (art. 5.1 c) del Reglamento Delegado (UE) 2025/301).

Si dicho plazo tiene lugar en día inhábil, se debe tener en cuenta la Q&A relacionada más adelante.

12. En caso de que el plazo de comunicación de un incidente grave tenga lugar en un día inhábil, ¿cómo debe procederse respecto al plazo de notificación?

Cuando el plazo para la presentación de una notificación inicial, un informe intermedio o un informe final coincida con un fin de semana o con un día festivo en el Estado miembro de la entidad financiera notificante, **esta podrá efectuar dicha presentación hasta el mediodía del siguiente día hábil** (art. 5.4 del Reglamento Delegado (UE) 2025/301)[24].

Lo anterior, no se aplicará a la presentación de una notificación inicial o un informe intermedio por parte de entidades de crédito, entidades de contrapartida central, gestores de centros de negociación y otras entidades financieras identificadas como esenciales o importantes de conformidad con el artículo 3 de la Directiva (UE) 2022/2555 (art. 5.5 del Reglamento Delegado (UE) 2025/301). El informe final sí que se podrá presentar hasta el mediodía del siguiente día hábil para estas entidades.

13. ¿Qué ocurre en aquellas situaciones dónde la entidad financiera no pueda presentar por motivos técnicos alguna de las notificaciones requeridas?

Las entidades financieras que no puedan presentar la notificación inicial, el informe intermedio o el informe final en los plazos establecidos conforme al artículo 5.1 del Reglamento Delegado (UE) 2025/301, **informarán de ello a la autoridad competente** sin demora indebida pero a más tardar en los plazos respectivos para la presentación de la notificación o el informe, y explicarán los motivos del retraso (art. 5.3 del Reglamento Delegado (UE) 2025/301).

En el caso de las entidades obligadas a notificar a la CNMV no pudieran realizar alguna de las notificaciones deberán notificarlo al buzón de ciberseguridad (ciberseguridad@cnmv.es), indicando los motivos, la identificación de la entidad o entidades obligadas bajo DORA y datos de contacto.

14. ¿Por qué es importante notificar un incidente grave en plazo?

Si una entidad no notifica un incidente grave dentro del plazo establecido por el Reglamento DORA, **incurre en el incumplimiento de sus obligaciones en materia de gestión y notificación de incidentes**, lo que puede dar lugar a requerimientos de explicación, medidas correctoras o sanciones administrativas por parte de la autoridad competente (art. 50 y 51 del Reglamento DORA).

[24] Salvo que la autoridad competente decida no aplicarlo, en el caso de que la entidad sea significativa o tenga un carácter sistémico para el sector financiero a escala nacional o de la Unión. En este caso la autoridad se lo notificaría a la entidad (art. 5.6 del Reglamento Delegado (UE) 2025/301).

Además, la notificación fuera de plazo puede afectar a la coordinación sectorial ante incidentes significativos comprometiendo la resiliencia y estabilidad del sistema financiero.

Estas situaciones se deben evitar con una buena gobernanza e implementación del procedimiento de gestión de incidentes por parte de la entidad, estando preparada y minimizando el impacto (tanto económico como reputacional).

Por lo tanto, se recomienda a las entidades notificar el incidente a la autoridad en plazo, aunque haya dificultad al rellenar alguno de los campos, para cumplir con las obligaciones del Reglamento. Desde el buzón de ciberseguridad (ciberseguridad@cnmv.es) la CNMV puede ayudar si hay dudas sobre el Reglamento.

15. En relación con la notificación de incidentes graves en el marco del Reglamento DORA ¿puede realizarse de forma agregada para todo el grupo o debe realizarse de forma individual por cada entidad legal sujeta al Reglamento?

La obligación de notificar incidentes graves se aplica a cada entidad legal sujeta al Reglamento sin que se contemple la presentación consolidada de informes a nivel de grupo.

En el caso de externalización de las obligaciones de notificación como se indica en el artículo 19.5 del Reglamento DORA (incluyendo la externalización a un proveedor intragrupo), el artículo 7 del Reglamento de Ejecución (UE) 2025/302 permite proporcionar información agregada sobre un incidente que afecte a varias entidades financieras en una única notificación o informe, siempre y cuando se cumplan todas las condiciones del artículo 7.1 del citado reglamento.

Por consiguiente, como regla general, cada entidad deberá realizar la notificación de incidentes graves ante la autoridad competente que corresponda.

Para evitar duplicidades en la gestión y seguimiento de las notificaciones, se recomienda que la entidad indique, en los campos previstos para ello (por ejemplo, los campos 2.10 y 3.31 del formulario), las demás autoridades, distintas a la CNMV, a las que otras entidades del grupo también hayan remitido el informe debido al mismo incidente.

16. ¿Tiene la entidad financiera obligación de notificar a sus clientes la existencia de un incidente grave relacionado con las TIC que afecte a sus servicios?

Sí. Cuando el incidente grave relacionado con las TIC tenga consecuencias para los intereses financieros de los clientes, las entidades financieras informarán a sus clientes, sin demora indebida, de dicho incidente tan pronto como tengan conocimiento del mismo y les comunicarán todas las medidas que se hayan adoptado para mitigar sus efectos adversos. (art. 19.3 del Reglamento DORA).

En caso de ciberamenaza importante, las entidades financieras informarán, cuando proceda, a aquellos clientes que pudieran verse afectados de cualquier medida de protección adecuada que estos consideren oportuno adoptar (art. 19.3 del Reglamento DORA).

El proceso de gestión de incidentes deberá incluir planes para la notificación a los clientes (art. 17.3.d) del Reglamento DORA).

17. Además de las notificaciones mencionadas, ¿hay otras obligaciones cuando ocurre un incidente grave relacionado con las TIC?

El artículo 17.3.e) del Reglamento DORA establece que, al menos los incidentes graves, se deben poner en conocimiento de los altos directivos pertinentes e informar al Consejo de Administración, explicando sus repercusiones, las medidas adoptadas como respuesta y los controles adicionales que se prevé implantar como resultado de estos incidentes graves relacionados con las TIC.

Además, las entidades deberán revisar su marco de gestión de riesgos TIC tras un incidente grave para determinar y evaluar los riesgos relacionados con las TIC y la seguridad de la información e identificar las mejoras necesarias (art. 13.2 del Reglamento DORA y 31.1.e) del Reglamento Delegado (UE) 2024/1774).

18. ¿Qué ocurre si un incidente categorizado previamente como grave pasa a ser considerado como un incidente no grave?

Cuando, tras una nueva evaluación, la entidad financiera concluya que el incidente relacionado con las TIC notificado previamente como grave no cumplía en ningún momento los criterios y umbrales de clasificación establecidos en el artículo 8 del Reglamento Delegado (UE) 2024/1772, notificará a la autoridad competente que ha reclasificado el incidente relacionado con las TIC de grave a no grave facilitando la información sobre dicha reclasificación en la plantilla que figura en el anexo II del Reglamento de Ejecución (UE) 2025/302 en relación con los campos «tipo de informe» y «otra información».

19. ¿Puede externalizarse la obligación de notificación de un incidente grave relacionado con las TIC?

Sí. Las entidades financieras podrán externalizar las obligaciones de información de incidentes graves a su autoridad a un proveedor tercero de servicios. No obstante, la entidad financiera seguirá siendo plenamente responsable del cumplimiento de los requisitos en materia de notificación de incidentes (art. 19.5 del Reglamento DORA).

En relación con lo anterior, conforme al artículo 6 del Reglamento de Ejecución (UE) 2025/332, las entidades financieras que hayan externalizado la obligación de notificar incidentes graves informarán a su autoridad competente de dicho acuerdo de externalización tan pronto como se haya celebrado este y, a más tardar, antes de la primera notificación o informe.

Además, las entidades financieras facilitarán a la autoridad competente el nombre, los datos de contacto y el código de identificación del tercero que vaya a presentar las notificaciones de incidentes graves relacionados con las TIC o los informes correspondientes. Igualmente, las entidades financieras informarán a su autoridad competente tan pronto como dejen de externalizar estas obligaciones.

En el caso de las entidades financieras que deban notificar a la CNMV, el procedimiento de notificación de incidentes graves publicado en la web de la CNMV, sección de ciberseguridad[25], indica cómo realizar dicha comunicación.

20. ¿Las entidades deben hacer algo si les ocurre un incidente TIC que no se clasifique como grave?

[25] https://www.cnmv.es/Portal/Ciberseguridad

Las entidades, aunque no estén obligadas a notificar a la autoridad al no haberse clasificado como grave, deben seguir aplicando su proceso de gestión de incidentes TIC.

Tal y como indican los artículos 17.2, 17.3 y 18.1 del Reglamento DORA, las entidades financieras deben registrar y clasificar todos los incidentes y, en función de su criticidad y la causa subyacente, realizar un seguimiento, tratamiento y respuesta, tal y como establezca el proceso de gestión de incidentes de la entidad.

En muchas ocasiones una eficaz gestión del incidente evitará que se clasifique como grave (por ejemplo, si se acorta la duración de la caída del servicio o si se reduce su impacto económico o se evita un impacto reputacional).

21. ¿Las sucursales deben notificar los incidentes directamente o a través de su matriz?

En el caso de las sucursales, al no ser entidades jurídicas independientes, sino extensiones operativas de su entidad matriz, la responsabilidad de notificar los incidentes graves bajo el Reglamento DORA recae en la entidad principal. Dicha entidad legal debe tener en cuenta, en su proceso de gestión y notificación de incidentes TIC, la afectación a cualquiera de sus sucursales, independientemente del Estado miembro donde se encuentren.

La matriz deberá tener en cuenta el criterio de "extensión geográfica" a la hora de determinar los criterios para clasificar el incidente TIC como grave (Reglamento Delegado (UE) 2024/1772) y, si fuera el caso, rellenar la información relacionada con los países afectados correctamente en las notificaciones a la autoridad (campos 2.6, 3.18 y 3.19 del Reglamento de Ejecución (UE) 2025/302).

Si hay más de un Estado miembro afectado en la notificación del incidente grave, las correspondientes autoridades también recibirán ese informe a través de la Autoridad Europea de Supervisión correspondiente (ESMA, EBA o EIOPA) (art. 19.7 del Reglamento DORA).

22. En la notificación de un incidente grave bajo el Reglamento DORA ¿ los costes imputados de personal deben ser reportados como parte de los costes y pérdidas brutos directos e indirectos del incidente?

Las Autoridades Europeas de Supervisión han publicado la siguiente respuesta conjunta[26]:

El artículo 7.1.c) del Reglamento Delegado (UE) 2024/1772 especifica que el impacto económico de un incidente relacionado con las TIC incluye los costes de personal. La disposición también especifica que los costes del personal incluyen los costes "asociados a la sustitución o reubicación de personal, la contratación de personal adicional, la remuneración de horas extra y la recuperación de habilidades perdidas o deterioradas". Cuando las horas extra no se remuneran, sino que se compensan mediante acuerdos de tiempo de trabajo, las horas extras relacionadas con el incidente deberían seguir contando para los costes del personal, siempre que esos costes puedan atribuirse claramente al incidente. De igual modo, ***el tiempo de trabajo claramente asignado a la gestión del incidente debería contar para los costes del personal****. Esta consideración también se aplica cuando los* ***recursos han sido destinados o planificados para la gestión de incidentes en general****. Esto garantiza una evaluación coherente de los costes independientemente de los procesos internos y la planificación y asignación de recursos de las entidades financieras.*

[26] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2025_7439

Las actividades de formación del personal destinadas a prevenir o minimizar las consecuencias de posibles incidentes están excluidas de los costes conforme al artículo 7.2) del Reglamento Delegado (UE) 2024/1772 para mantener actualizadas las competencias del personal, como coste necesario para la operación diaria del negocio. En cambio, los costes para recuperar habilidades perdidas o deterioradas son aquellos que ocurren como consecuencia de un incidente conforme al artículo 7(1) del Reglamento Delegado (UE) 2024/1772, por ejemplo, que aborda la reformación del personal que tuvo que ser reasignada.

Cabe señalar que el Reglamento de Delegado (UE) 2024/1772 no prescribe una metodología de cálculo específica para estos costes. Esta omisión refleja la complejidad inherente y la variabilidad de las estructuras de costes entre diferentes entidades y actividades financieras.

23. ¿Qué buenas prácticas pueden reforzar la gestión de incidentes TIC?

Para reforzar el cumplimiento del pilar de gestión de incidentes previsto en el Reglamento DORA, las entidades financieras pueden adoptar un conjunto de **buenas prácticas** organizativas, procedimentales y tecnológicas orientadas a garantizar una detección temprana, una comunicación eficaz y una respuesta coordinada. Entre las principales destacan las siguientes:

1. **Definir procedimientos internos claros y normalizados** para la gestión y notificación de incidentes TIC, aprobados por la dirección, asegurando que incluyan criterios de clasificación, umbrales de gravedad y canales de comunicación definidos con antelación.
2. **Establecer roles y responsabilidades precisos**, incluyendo la designación de un responsable o equipo específico de coordinación de incidentes, con conexión directa a la función de seguridad, cumplimiento y alta dirección.
3. **Alinear los procesos internos con los plazos y formatos establecidos** por el Reglamento DORA y sus normas técnicas, priorizando la capacidad de generar informes de notificación (inicial, intermedio y final) de forma automatizada o semiautomatizada.
4. **Implantar herramientas de monitorización y detección temprana** (SIEM, IDS/IPS, EDR, SOC interno o gestionado), que permitan identificar comportamientos anómalos y facilitar la trazabilidad de los incidentes.
5. **Realizar simulacros y ejercicios periódicos** de notificación y gestión de crisis, que involucren tanto a los equipos técnicos como a las áreas de dirección de negocio, comunicación y cumplimiento, con el fin de verificar la eficacia del procedimiento.
6. **Promover la cultura de reporte interno**, asegurando que cualquier empleado o proveedor pueda comunicar rápidamente un incidente o indicio, fomentando así la detección temprana.
7. **Integrar los aprendizajes posteriores a cada incidente** (“*lecciones aprendidas*”) en la mejora continua del proceso de notificación, revisando los indicadores de rendimiento y los tiempos de respuesta.

8. **Coordinar la notificación** con terceros críticos y proveedores de servicios de TIC. Establecer cláusulas contractuales claras de notificación de incidentes y ejercicios conjuntos de gestión de incidentes.
9. **Asegurar la comunicación fluida con las autoridades competentes**, manteniendo los contactos actualizados y verificando la capacidad técnica para transmitir notificaciones de acuerdo con los canales seguros designados por el supervisor.

En conjunto, estas prácticas fortalecen la capacidad de la entidad para detectar, comunicar y gestionar incidentes TIC de forma ágil, trazable y conforme al Reglamento DORA, reduciendo tanto el impacto operativo como el riesgo reputacional.

Pruebas de resiliencia operativa digital

1. ¿Cuál es la naturaleza y objetivo principal de las pruebas de resiliencia operativa y digital según el Reglamento DORA?

Las entidades financieras que no sean microempresas establecerán, mantendrán y revisarán, teniendo en cuenta los criterios de proporcionalidad establecidos en el artículo 4.2 del Reglamento DORA, un **programa de pruebas de resiliencia operativa digital** sólido y completo que forme parte del marco de gestión del riesgo relacionado con las TIC al que se refiere el artículo 6 del mencionado Reglamento.

Las microempresas también planificarán pruebas de ciberresiliencia, con un enfoque basado en riesgo, teniendo en cuenta su capacidad y otros factores relevantes, como el tipo de riesgo, la esencialidad de los activos de información y los servicios prestados (art. 25.3 del Reglamento DORA).

El objetivo principal de las pruebas de resiliencia operativa y digital establecidas en el Reglamento DORA reside en evaluar y fortalecer la capacidad de una entidad financiera para resistir, responder y recuperarse eficazmente ante incidentes que afecten a los sistemas y servicios de TIC que sustenten funciones esenciales o importantes.

Estas pruebas permiten comprobar, de forma controlada y periódica, la robustez de los controles técnicos, los procedimientos operativos y los planes de contingencia, identificando vulnerabilidades o deficiencias que podrían comprometer la continuidad de los servicios esenciales o importantes de la entidad.

Este principio se recoge en el artículo 24 del Reglamento DORA, que obliga a las entidades financieras (no microempresas) a establecer un programa de pruebas de resiliencia operativa digital proporcionado, basado en el riesgo y actualizado de forma regular.

2. ¿Con qué frecuencia deben realizarse las pruebas de resiliencia?

Las entidades financieras deben realizar las pruebas de resiliencia operativa digital de forma periódica y proporcionada al nivel de riesgo, asegurando que el programa de pruebas se revise y actualice regularmente (art. 24 del Reglamento DORA).

Aunque el Reglamento no establece una periodicidad única para todas las entidades, si establece que las entidades financieras que no sean microempresas efectúen, **al menos una vez al año**, las pruebas apropiadas de todos los sistemas y aplicaciones de TIC que sustenten funciones esenciales o importantes.

Adicionalmente, el Reglamento contempla la realización de pruebas avanzadas basadas en amenazas (Threat-Led Penetration Testing, **TLPT**) que están dirigidas a entidades maduras, las cuales deberán ejecutarse **al menos en periodos de tres años**, conforme al Reglamento Delegado (UE) 2025/1190 que desarrolla el artículo 26 del Reglamento DORA.

3. ¿Qué tipos de pruebas de resiliencia operativa digital contempla el Reglamento DORA?

El programa de pruebas de resiliencia operativa digital al que se refiere el artículo 24 del Reglamento DORA dispondrá, de conformidad con los criterios establecidos en el artículo 4.2, la ejecución de pruebas adecuadas, como evaluaciones y exploraciones de vulnerabilidad, análisis del software de código abierto, evaluaciones de seguridad de la red, análisis de

carencias, exámenes de la seguridad física, cuestionarios y soluciones de software de detección, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo y pruebas de penetración (art. 25.1 del Reglamento DORA).

Hay otro tipo de pruebas, relacionadas con la ciberresiliencia, que se mencionan expresamente, como las pruebas del **plan de continuidad** y **medidas de respuesta y recuperación** (arts. 11.6 y 16.1.g) del Reglamento DORA y art. 25 del Reglamento Delegado (UE) 2024/1774) y en la **adquisición, desarrollo y mantenimiento** de sistemas TIC (arts.16 y 37 del Reglamento Delegado (UE) 2024/1774).

Además, las entidades a las que no les aplique el marco simplificado de gestión de riesgos TIC, deberán probar los **planes de comunicación** (art. 11.6.b) del Reglamento DORA), realizar pruebas **en entornos de desarrollo y de producción** (arts. 8.2, 15.3.g) y 16.2 del Reglamento Delegado (UE) 2024/1774), y en el proceso de **gestión de cambios** TIC (art.17.1.c) del Reglamento Delegado (UE) 2024/1774).

Cada entidad deberá valorar las pruebas que son más adecuadas según su madurez y riesgos TIC detectados. Por ejemplo, la exposición a ataques de phishing por los empleados, la madurez de la dirección para tomar decisiones en situaciones de crisis, escenarios de restauración de datos o sistemas ante ataques de ransomware, la capacidad de probar la redundancia ante fallos de sistemas, etc.

En el caso de pruebas de ciberseguridad, se va madurando desde los **escaneos de vulnerabilidades** (con herramientas automáticas priorizando los servicios expuestos a Internet), evolucionando a las pruebas de **pentesting** (más manuales, donde se escanea e intenta explotar las vulnerabilidades detectadas para ver posibles movimientos laterales a otros sistemas) y, si se tiene la suficiente madurez y recursos, llegar a realizar pruebas de **red teaming** (una simulación de ataque más realista donde sólo una parte de la entidad conoce la prueba para probar la capacidad de detección y respuesta).

4. ¿Qué función debe ser la encargada de realizar las pruebas de resiliencia operativa digital en una entidad financiera según el Reglamento DORA?

Las entidades financieras que no sean microempresas **garantizarán que las pruebas sean realizadas por partes independientes**, ya sean internas o externas. Cuando un probador interno se encargue de realizar las pruebas, las entidades financieras dedicarán recursos suficientes y **garantizarán que se evitan los conflictos de intereses** durante todas las fases de constitución y ejecución de las pruebas (art. 24.4 del Reglamento DORA).

Para las entidades más pequeñas, más limitades en recursos, es fundamental que la función de control, al ser independiente, revise que estas pruebas se realicen periódicamente, acorde con los planes, políticas y procedimientos aprobados por la entidad y se haga un seguimiento de los resultados de todo el trabajo realizado por la función de gestión correspondiente.

5. En relación con el desarrollo de pruebas de resiliencia digital, ¿existen diferencias o excepciones teniendo en cuenta la naturaleza de las entidades financieras?

Sí. **Los depositarios centrales de valores y las entidades de contrapartida central** realizarán evaluaciones de vulnerabilidad antes de implantar o reimplantar aplicaciones y componentes de infraestructuras y servicios de TIC que sustenten funciones esenciales o importantes de la entidad financiera nuevos o ya existentes (art. 25.2 del Reglamento DORA y arts. 8.2, 15.2.g del

Reglamento Delegado (UE) 2024/1774) y otras pruebas dentro de su marco de gestión de riesgos (arts. 16.2, 17.2, 25.3 y 25.4 del Reglamento Delegado (UE) 2024/1774).

Además, **las microempresas** realizarán las pruebas a las que se refiere el artículo 25.1 del Reglamento DORA mediante la combinación de un enfoque basado en el riesgo con una planificación estratégica de las pruebas de TIC, teniendo debidamente en cuenta la necesidad de mantener un planteamiento equilibrado entre la dimensión de los recursos y el tiempo que se asigne a las pruebas de TIC previstas en el presente artículo, por una parte, y la urgencia, el tipo de riesgo, el carácter esencial de los activos de información y de los servicios prestados, así como cualquier otro factor pertinente, incluida la capacidad de la entidad financiera para asumir riesgos calculados, por otra (art. 25.3 del Reglamento DORA). Las microempresas también están exentas de i) realizar las pruebas por partes independientes, ii) establecer procedimientos y políticas para hacer un seguimiento exhaustivo del resultado de las pruebas y iii) a realizar pruebas anuales de todos los sistemas y aplicaciones TIC que sustenten funciones esenciales o importantes (arts. 25.4, 25.5 y 25.6 del Reglamento DORA).

Para las entidades a las que se les aplica el **marco simplificado de gestión de riesgos TIC**, se indica que deben establecer y aplicar un plan de pruebas de seguridad de las TIC, teniendo en cuenta el perfil de riesgo general de sus activos TIC (art. 36 del Reglamento Delegado (UE) 2024/1774).

6. ¿Qué entidades están obligadas a realizar pruebas de penetración basadas en amenazas (TLPT)?

Las autoridades competentes evaluarán si una entidad financiera está obligada a realizar pruebas de penetración basadas en amenazas teniendo en cuenta factores relacionados con la repercusión en el sistema financiero, sus posibles problemas de estabilidad financiera, incluido el carácter sistémico y su perfil de riesgo relacionado con las TIC. Los criterios de evaluación han sido definidos en los artículos 2.1 y 2.2 del Reglamento Delegado (UE) 2025/1190.

Las autoridades notificarán a las entidades financieras que resulten obligadas a realizar pruebas TLPT.

Hay que tener en cuenta que estas pruebas requieren un elevado nivel de madurez por parte de la entidad financiera, puesto que están dirigidas a sistemas TIC en producción que soportan funciones críticas de la entidad. Son costosas en recursos (en tiempo, en dinero y en personal dedicado). La autoridad supervisa todo el proceso para asegurar que se gestionen bien los riesgos durante el desarrollo de la prueba y se haga cumpliendo con los requisitos la normativa.

7. ¿Qué relación hay entre las pruebas TLPT y el marco TIBER-EU/TIBER-ES?

El marco **TIBER-EU** constituye el primer marco común a escala europea para la realización de pruebas de red. Si bien fue inicialmente concebido para entidades e infraestructuras financieras, TIBER-EU puede ser adoptado para su aplicación en cualquier tipo de entidad de cualquier sector. El objetivo del marco no es calificar como aprobada o suspensa a la entidad que se somete a las pruebas, sino mejorar el conocimiento de sus debilidades y fortalezas ante ciberataques e identificar medidas que incrementen su ciberresiliencia.

El marco **TIBER-ES** se adhiere a los principios de TIBER-EU, de manera que las pruebas realizadas bajo el primero garantizan el reconocimiento de las autoridades en otras jurisdicciones de la Unión Europea.

La CNMV es la autoridad designada para las pruebas TIBER-ES de las entidades financieras que supervisa, participando en todas las fases de la prueba, en colaboración con el Banco de España y la Dirección General de Seguros y Fondos de Pensiones.

Ambos marcos se han adaptado para que sus **guías de implementación** se adecúen a los requisitos de las pruebas TLPT referidas en los artículos 26 y 27 del Reglamento DORA y el Reglamento Delegado (UE) 2025/1190.

Por lo tanto, la CNMV utiliza las guías del marco TIBER-ES para el seguimiento de las pruebas de las entidades que supervisa y espera que la metodología y documentación de dichas pruebas esté alineada con dicho marco.

8. ¿Qué buenas prácticas pueden reforzar la realización de pruebas de resiliencia digital?

A continuación, se exponen una serie de buenas prácticas derivadas del Reglamento DORA y dirigidas a reforzar la realización de pruebas de resiliencia digital:

Planificación basada en riesgos: Diseñar el programa de pruebas end-to-end (frente a pruebas de componentes aislados) teniendo en cuenta el mapa de riesgos y la priorización de riesgos TIC, asegurando que se evalúen los sistemas y procesos que sustentan funciones esenciales o importantes (art. 24 del reglamento DORA).

Enfoque progresivo y proporcional: Ajustar el alcance y la complejidad de las pruebas al tamaño, perfil de riesgo y criticidad de la entidad, aplicando desde pruebas básicas de continuidad hasta ejercicios avanzados tipo TLPT.

Definición de objetivos y criterios claros: Establecer metas medibles, escenarios realistas y criterios de éxito que permitan identificar vulnerabilidades y áreas de mejora.

Participación de equipos multidisciplinares: Involucrar a las áreas de ciberseguridad, continuidad, negocio y gestión de riesgos para obtener una visión integral de la resiliencia y también contar con los proveedores TIC críticos en las pruebas.

Documentación y trazabilidad: Registrar el alcance, resultados y acciones derivadas de cada prueba, garantizando la trazabilidad y la capacidad de reporte ante las autoridades competentes.

Gestión de hallazgos y mejora continua: Establecer planes de remediación con plazos y responsables definidos, e incorporar los resultados de las pruebas en la actualización del marco de gestión de riesgos TIC.

En conjunto, estas buenas prácticas fortalecen la resiliencia operativa digital y ayudan a la entidad anticiparse a posibles disrupciones, mejorar sus capacidades de respuesta y cumplir con las exigencias regulatorias del Reglamento DORA en materia de pruebas de resiliencia.

Gestión del riesgo relacionado con las TIC derivado de terceros

1. ¿Qué tipos de servicios deben considerarse servicios de TIC y cuáles servicios financieros según el Reglamento DORA?

La definición de servicios de TIC debe entenderse de manera amplia en la medida en que dichos servicios abarquen los servicios digitales y de datos prestados a través de sistemas de TIC de forma continua. Por lo tanto, las entidades financieras son responsables de realizar una evaluación sobre esta base para determinar si los servicios en los que confían son servicios de TIC (art. 3.21 del Reglamento DORA). Dicha evaluación debe realizarse teniendo en cuenta las aclaraciones del considerando 63 del Reglamento DORA, que especifica que DORA debe abarcar una amplia gama de proveedores terceros de servicios de TIC, incluidas las entidades financieras que prestan servicios de TIC a otras entidades financieras, y sin perjuicio de las regulaciones sectoriales aplicables a los servicios financieros regulados.

En caso de que el servicio sea prestado por una entidad financiera regulada que preste servicios financieros regulados, pero dicho servicio no esté relacionado o sea independiente de los servicios financieros regulados, el servicio debe considerarse un servicio de TIC bajo DORA.

El mismo razonamiento se aplica a los servicios auxiliares prestados por una entidad, dependiendo de si dichos servicios auxiliares son servicios financieros regulados o un servicio necesario para la prestación de un servicio financiero regulado, y no se prestan de forma independiente.

Esta aclaración sobre la diferencia entre los servicios financieros y los servicios de TIC se realiza sin perjuicio de los requisitos que son de aplicación para las entidades financieras según el Reglamento DORA, salvo los requisitos relacionados con la gestión de riesgos de terceros de TIC[27].

2. ¿Qué diferencia hay entre los proveedores esenciales de servicios de TIC y los proveedores de servicios de TIC que sustentan funciones esenciales o importantes?

Los proveedores esenciales de servicios de TIC son los proveedores de servicios de TIC que las Autoridades Europeas de Supervisión hayan designado como esenciales para las entidades financieras y le es aplicable el marco de supervisión previsto en el Reglamento DORA (Sección II, artículos 31 al 44 del Reglamento). Esta designación se basa en unos criterios que tienen en cuenta el impacto sistémico en la estabilidad y continuidad en la prestación de servicios para las entidades financieras y en la dependencia de las entidades respecto a los servicios prestados por el proveedor y el grado de sustituibilidad del proveedor de servicios de TIC.

Por otro lado, las entidades financieras deberán identificar los proveedores de servicios de TIC que sustenten sus funciones esenciales o importantes (ver glosario de términos). La relevancia de un proveedor para una entidad financiera no se determina únicamente por el tratamiento de datos de clientes o su relevancia sistémica, sino que se deberá tener en cuenta el impacto operacional, legal o reputacional que tendría una disrupción de su servicio en la entidad financiera.

[27] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en

Por lo tanto, un proveedor de servicios de TIC que sustente funciones esenciales e importantes para una entidad financiera también puede ser designado a nivel europeo como esencial.

3. ¿Qué implicaciones tiene el Reglamento DORA para los proveedores de servicios de TIC?

El Reglamento DORA es de aplicación directa a los proveedores de servicios de TIC designados como esenciales, a nivel europeo, al ser objeto de actividades de supervisión bajo el marco de supervisión establecido en los artículos 31 al 44 del Reglamento DORA.

Por otro lado, los proveedores de servicios de TIC, indirectamente, tienen que cumplir con una serie de obligaciones para que las entidades financieras no incumplan con el Reglamento DORA como, por ejemplo, determinadas clausulas en sus contratos derivadas del artículo 30.2 o tener un código de identificación LEI o EUID y otros datos para que la entidad pueda mantener el registro de proveedores de servicios de TIC (art. 28.3 del Reglamento DORA y el Reglamento de ejecución (UE) 2024/2956).

Si los proveedores, además, sustentan funciones esenciales en una entidad, tienen que cumplir con una serie de obligaciones adicionales para que las entidades financieras no incumplan con el Reglamento DORA (como, por ejemplo, un clausulado más exigente presente en el artículo 30.3 del Reglamento o cumplir con la política de contratación y subcontratación de la entidad referida en los Reglamentos Delegados (UE) 2024/1773 y 2025/532 respectivamente).

4. ¿Se deben incluir en el registro de información los proveedores de servicios de TIC que no sean esenciales para la entidad financiera?

Como parte de su marco de gestión del riesgo relacionado con las TIC, las entidades financieras 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 (art. 28.3 del Reglamento DORA).

Los acuerdos contractuales a que se refiere el párrafo primero se documentarán adecuadamente, distinguiendo entre los que comprendan servicios de TIC que sustentan funciones esenciales o importantes y los que no (art. 28.3 del Reglamento DORA).

La CNMV espera que, aplicando el principio de proporcionalidad, las entidades pongan el foco y prioricen los proveedores de servicios de TIC que sustenten las funciones esenciales o importantes y la cadena de contratación más relevante para prestar dicho servicio.

5. ¿Qué obligación de notificación y reporte a la autoridad tienen las entidades respecto al registro de información de los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC?

El artículo 28.3 establece tres obligaciones de las entidades financieras con su autoridad:

- Informar oportunamente cuando se propongan celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.
- Comunicar, al menos, una vez al año información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios

de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.

- Cuando la autoridad lo solicite, el registro completo de información o, cuando así se solicite, secciones específicas de este, junto con toda información que se considere necesaria para permitir la supervisión efectiva de la entidad financiera.

La CNMV ha publicado en su sección web de ciberseguridad la manera de informar cuando una entidad se proponga a firmar un nuevo acuerdo. Esta obligación es similar a las Directrices de ESMA de notificar ante la externalización de servicios en la nube, ampliándose el alcance a la contratación de cualquier servicio TIC que sustente funciones esenciales o importantes.

Para el segundo y tercer punto, la CNMV requiere con carácter anual el envío del registro completo de proveedores a sus entidades supervisadas que es aplicable el Reglamento DORA (con los datos de referencia del 31 de diciembre del año previo, para enviarlo a las Autoridades Europeas de Supervisión antes del 31 de marzo para la designación de los proveedores esenciales)[28].

6. ¿La adquisición de licencias de software on-premise deben tratarse como la provisión de un servicio TIC sujeto al Reglamento DORA?

La CNMV considera que no tendría esa consideración de proveedor de servicio TIC, cuando las licencias de software on-premise constituyen un contrato puntual de adquisición (sin una fecha de finalización del servicio), tratándose por tanto de una mera transacción. Normalmente, dichas licencias pueden incluir beneficios adicionales, como actualizaciones de seguridad durante el ciclo de vida de la versión o acceso a un canal de soporte oficial. No obstante, este riesgo puede gestionarse dentro del marco general de gestión de riesgos tecnológicos —por ejemplo, mediante la gestión de vulnerabilidades o el seguimiento del ciclo de vida del software— sin necesidad de aplicar íntegramente los requisitos propios de la gestión de proveedores de servicios de TIC (SLAs, monitorización, registro, etc.). En cambio, un contrato marco de tipo “Enterprise Agreement”, que tenga duración determinada y contemple la actualización continuada de versiones de productos, sí podría considerarse un servicio TIC sujeto a las obligaciones establecidas por DORA.

7. ¿Como deben actuar las entidades financieras a la hora de celebrar un acuerdo contractual según el Reglamento DORA?

Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, las entidades financieras (art. 28.4 del Reglamento DORA):

a) Evaluarán si el acuerdo contractual se refiere al uso de servicios de TIC que sustenten una **función esencial o importante**.
b) Evaluarán si se cumplen las **condiciones de supervisión** para la contratación.
c) Determinarán y evaluarán todos **los riesgos pertinentes** en relación con el acuerdo contractual, incluida la posibilidad de que dicho acuerdo pueda contribuir a reforzar el riesgo de concentración de TIC a que se refiere el artículo 29 del Reglamento DORA.

[28] Estos plazos se ajustan al anuncio de las AES sobre el calendario para recibir el registro de información de proveedores bajo DORA. Si este calendario se modifica, la CNMV actualizaría sus procedimientos en la web de la CNMV, sección de ciberseguridad.

d) Llevarán a cabo todas las **comprobaciones debidas** con respecto a los posibles proveedores terceros de servicios de TIC y se asegurarán, a través de los procesos de selección y evaluación, de la idoneidad de dichos proveedores.
e) Determinarán y evaluarán los **conflictos de intereses** que el acuerdo contractual pueda causar.

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. (art. 28.5 del Reglamento DORA).

Siendo DORA un Reglamento de reciente aplicación, la CNMV entiende que al principio haya proveedores que no cumplan con todos los requisitos del Reglamento en los contratos vigentes. La CNMV espera que las entidades financieras valoren los riesgos y, de manera proporcional, evalúen la dependencia con el proveedor, el grado de sustituibilidad y el impacto de finalización del contrato. Siendo un reglamento que es aplicable para todo el sector financiero en Europa, se espera que los proveedores, cada vez más, colaboren con las entidades financieras y las autoridades para poder dar servicio a este sector.

8. ¿En qué condiciones puede un proveedor tercero de servicios de TIC hacer uso de subcontratistas que sustenten funciones esenciales o importantes?

Antes de celebrar un acuerdo contractual con un proveedor tercero de servicios de TIC, que sustente funciones esenciales o importantes, la entidad financiera determinará si dicho proveedor podría a su vez subcontratar dichos servicios, o partes sustanciales de ellos.

La entidad financiera solo celebrará dicho acuerdo contractual si considera que el proveedor tercero de servicios de TIC es capaz de seleccionar y evaluar las capacidades operativas y financieras de los posibles subcontratistas de TIC, identificar dichos subcontratistas e informar de ellos a la entidad financiera proporcionando toda la información que pueda ser necesaria para evaluar las condiciones requeridas. Además, el proveedor tercero de servicios de TIC debe garantizar que los acuerdos contractuales con los subcontratistas permitan a la entidad financiera cumplir sus propias obligaciones derivadas del Reglamento DORA y de la legislación nacional y de la Unión aplicable.

El subcontratista debe conceder a la entidad financiera y a las autoridades competentes y de resolución los mismos derechos contractuales de acceso e inspección que los concedidos por el proveedor tercero de servicios de TIC. Sin perjuicio de la responsabilidad final de la entidad financiera de cumplir sus obligaciones jurídicas y normativas, se espera que el propio proveedor tercero de servicios de TIC tenga capacidad, conocimientos especializados y recursos suficientes para llevar a cabo un seguimiento de los riesgos de TIC de los subcontratistas.

La entidad financiera evaluará si las cadenas de subcontratación potencialmente largas o complejas pueden afectar a su capacidad para efectuar un seguimiento completo de las funciones contratadas y a la capacidad de la autoridad competente para supervisar efectivamente a la entidad financiera a este respecto, y de qué manera.

En definitiva, se espera que la entidad financiera tenga la misma capacidad de evaluación y control sobre los subcontratistas que sobre el proveedor de terceros TIC (art. 3 del Reglamento Delegado (UE) 2025/532).

9. ¿Qué se espera de un proveedor de servicios de TIC que subcontrate funciones esenciales o importantes, o partes sustanciales de ellas?

El proveedor tercero de servicios de TIC es responsable de los servicios prestados por los subcontratistas, además está obligado a supervisar todos los servicios de TIC subcontratados que sustenten funciones esenciales o importantes, o partes sustanciales de ellas, a fin de garantizar el cumplimiento continuado de sus obligaciones contractuales con la entidad financiera. Además, se espera que el proveedor tercero de servicios de TIC evalúe todos los riesgos asociados a la ubicación de los subcontratistas actuales o potenciales que presten servicios de TIC que sustenten funciones esenciales o importantes, o partes sustanciales de ellas, a su sociedad matriz y a la ubicación desde la que se presta el servicio de TIC subcontratado (art. 4 del Reglamento Delegado (UE) 2025/532).

El proveedor tercero de servicios de TIC debe especificar en el contrato que formalice con sus subcontratistas todas las obligaciones derivadas del Reglamento DORA y el Reglamento Delegado (UE) 2025/532. De igual forma, se espera que el proveedor tercero de servicios de TIC notifique a la entidad financiera cualquier cambio significativo introducido en los acuerdos de subcontratación (art. 5 del Reglamento Delegado (UE) 2025/532).

10. ¿En qué condiciones se contempla la terminación del contrato entre la entidad financiera y el proveedor tercero de servicios de TIC?

Las entidades financieras deben garantizar la posibilidad de terminar los acuerdos contractuales sobre el uso de servicios de TIC en cualquiera de los siguientes casos (art. 28.7 del Reglamento DORA):

- I**ncumplimiento importante** por parte del proveedor tercero de servicios de TIC de las disposiciones legales o reglamentarias o las cláusulas contractuales aplicables.
- Circunstancias observadas durante el seguimiento del riesgo relacionado con las TIC derivado de terceros que se considere que pueden **alterar el desempeño** de las funciones prestadas en virtud del acuerdo contractual, incluidos cambios importantes que afecten al acuerdo o a la situación del proveedor tercero de servicios de TIC.
- **Debilidades manifiestas** del proveedor tercero de servicios de TIC en cuanto a su gestión global del riesgo relacionado con las TIC y, en particular, a la forma en que garantiza la disponibilidad, la autenticidad, la integridad y la confidencialidad de los datos, ya sean personales o sensibles en cualquier otro sentido, o no personales.
- Cuando **la autoridad competente** haya dejado de poder supervisar efectivamente a la entidad financiera como resultado de las condiciones del acuerdo contractual o circunstancias relacionadas con él.

11. ¿En qué condiciones se contempla la terminación del contrato entre la entidad financiera y el proveedor tercero de servicios de TIC en relación con la subcontratación de servicios?

La entidad financiera deberá incluir en el acuerdo contractual la especificación de terminación del contrato cuando concurra alguna de las situaciones siguientes (art. 6 Reglamento Delegado (UE) 2025/532):

- La entidad financiera **se haya opuesto a la introducción de cambios** sustanciales en los acuerdos de subcontratación que sustenten funciones esenciales o importantes y haya solicitado modificar dichos acuerdos, pero el proveedor tercero de servicios de TIC haya aplicado, no obstante, tales cambios sustanciales.

- El proveedor tercero de servicios de TIC **introduce cambios sustanciales en los acuerdos de subcontratación** que sustenten funciones esenciales o importantes, o partes sustanciales de ellas sin la aprobación de la entidad financiera.
- El proveedor tercero de servicios de TIC **subcontrate un servicio TIC** que sustente una función esencial o importante, o partes sustanciales de ellas, que no esté expresamente permitido subcontratar en virtud del contrato formalizado entre la entidad financiera y el proveedor tercero de servicios de TIC.

12. ¿Qué ocurre si un proveedor tercero de servicios de TIC está establecido en un tercer país?

En estos casos, las entidades financieras tendrán en consideración el cumplimiento de la normativa en materia de protección de datos de la Unión y la aplicación efectiva del Derecho en ese tercer país (art. 29.2 del Reglamento DORA).

Además, las entidades financieras deben ponderar los beneficios y los riesgos que puedan derivarse de la posible subcontratación, en particular cuando se trate de un subcontratista de TIC establecido en un tercer país.

Dados los riesgos geopolíticos y su afectación en las cadenas de suministro, cada vez resulta más relevante perseguir una mayor soberanía digital a nivel español y/o europeo.

13. ¿Qué debe hacer una entidad si depende en exceso de un solo proveedor de servicios de TIC?

Las entidades financieras ponderarán los beneficios y los costes de soluciones alternativas, como el recurso a distintos proveedores terceros de servicios de TIC, considerando si las soluciones contempladas se ajustan a las necesidades y objetivos empresariales establecidos en su estrategia de resiliencia digital y de qué manera (art. 29.1 del Reglamento DORA).

La CNMV espera, en la medida de lo posible, que las entidades financieras eviten la concentración de proveedores de servicios de TIC debido al riesgo que conlleva. En todo caso, si la entidad no tiene la capacidad para realizar un control a nivel técnico del servicio, se recomienda contratar un servicio independiente que le ayude a realizar una monitorización y seguimiento de sus proveedores más críticos.

14. ¿En qué consiste el proceso de diligencia debida recogido en el Reglamento DORA y el Reglamento Delegado (UE) 2024/1773?

La celebración formal de acuerdos contractuales debe fundarse e ir precedida de un análisis exhaustivo previo a la contratación, centrado en particular en elementos como el carácter esencial o la importancia de los servicios cubiertos por el contrato de TIC previsto, las aprobaciones de las autoridades de control necesarias u otras condiciones, el posible riesgo de concentración que conlleva, aplicando asimismo la diligencia debida en el proceso de selección y evaluación de los proveedores terceros de servicios de TIC y evaluando los posibles conflictos de intereses (Considerando 66 del Reglamento DORA).

La política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC, establecerá un proceso adecuado y proporcionado para la selección y evaluación de los posibles proveedores terceros de servicios de TIC, teniendo en cuenta si estos son o no proveedores intragrupo de servicios de TIC, y exigirá que la entidad financiera evalúe, antes de celebrar un acuerdo contractual, si el

proveedor tercero de servicios de TIC cumple con los requisitos expuestos en el artículo 6 del Reglamento Delegado (UE) 2024/1773 (auditorías, certificaciones y otras informaciones disponibles que garanticen que el proveedor alcanza el nivel de garantía requerido).

18. Un proveedor de servicios TIC está certificado en la ISO 27001 (u otra certificación equivalente), ¿cumple por lo tanto con el Reglamento DORA?

La certificación ISO 27001 (u otra certificación equivalente), certifica el cumplimiento de un conjunto de prácticas estándar de ciberseguridad, y normalmente no están adaptadas a las obligaciones del Reglamento DORA, por lo que su certificación no garantiza el cumplimiento con dicho reglamento al usar otro marco de referencia (por ejemplo, la certificación no tiene por qué validar si la entidad notifica a la entidad de los incidentes graves en plazo u otros requisitos derivados del clausulado contemplados en el artículo 30 del Reglamento DORA).

Dentro del proceso diligencia debida, las certificaciones de terceros sí que pueden constituir uno de los elementos adecuados para garantizar la idoneidad del proveedor, aunque indica que, cuando proceda, las entidades deben de utilizar elementos adicionales (art. 6.3 del Reglamento Delegado (UE) 2024/1773).

Por lo tanto, la CNMV espera que, antes de celebrar un acuerdo contractual, la entidad financiera valore, de manera proporcional, la idoneidad de un proveedor para prestar servicios de TIC (art. 28.4 del Reglamento DORA).

15. ¿Qué papel tiene una entidad financiera cuyos servicios de TIC se proporcionan desde la matriz del grupo (proveedores intragrupo)?

Los proveedores intragrupo de servicios de TIC, incluidos los que sean propiedad plena o colectiva de entidades financieras dentro del mismo sistema institucional de protección, deben considerarse proveedores terceros de servicios de TIC. Los riesgos que plantean los proveedores intragrupo de servicios de TIC pueden ser diferentes, pero los requisitos que les resultan aplicables en virtud del Reglamento DORA son los mismos. De manera similar, la política debe ser aplicable a los subcontratistas que presten servicios de TIC que sustenten funciones esenciales o importantes, o partes sustanciales de ellas, a proveedores terceros de servicios de TIC, cuando exista una cadena de proveedores terceros de servicios de TIC (Considerando 5 del Reglamento Delegado (UE) 2024/1773 y Considerando 63 del Reglamento DORA).

Por lo tanto, se espera que se firme un acuerdo que cumpla el clausulado del artículo 30 del Reglamento DORA (puede ser bajo un acuerdo marco de servicios) y se incluya en el registro de información de proveedores y las principales cadenas de contratación, entre otros.

La responsabilidad última del cumplimiento del Reglamento recae en el Consejo de Administración de la entidad financiera, por lo que la CNMV espera que, entre otras medidas: el Consejo de Administración se mantenga periódicamente informado de los riesgos TIC que le afecten a su entidad, si la entidad adopta las políticas procedimientos y planes del grupo, su implementación incluirá claramente las funciones de la propia entidad (con niveles de servicio y objetivos de recuperación adecuados) y que en las pruebas que se realicen a nivel de grupo incluyan los sistemas de la entidad financiera. La entidad financiera debe mantener los conocimientos técnicos necesarios para poder tener suficiente autonomía en la toma de decisiones sobre los riesgos TIC de la entidad que le afectan.

16. ¿Qué buenas prácticas pueden reforzar la gestión de riesgo de terceros según DORA?

A continuación, se exponen una serie de buenas prácticas derivadas del Reglamento DORA y dirigidas a reforzar la gestión del riesgo derivado de terceros proveedores de servicios de TIC:

Inventario y clasificación de proveedores de servicios de TIC: Mantener un registro actualizado de todos los terceros y subcontratistas, identificando aquellos que sustentan funciones esenciales o importantes (art. 8.5 y 8.6 del Reglamento DORA)

Evaluación previa y continua: Realizar análisis de riesgos antes de la contratación y evaluaciones periódicas sobre el desempeño, seguridad y cumplimiento del proveedor (art. 28.4 y 29 del Reglamento DORA)

Cláusulas contractuales claras: Incluir en los contratos aspectos exigidos por el Reglamento DORA (art. 28 y 30), como niveles de servicio, derechos de acceso, auditoría e información, requisitos de notificación de incidentes y localización de datos.

Monitorización y supervisión continua: Implementar mecanismos para vigilar el cumplimiento de los acuerdos, la gestión de incidentes y la estabilidad financiera y operativa del proveedor.

Planes de salida y contingencia: Definir estrategias de salida y sustitución que aseguren la continuidad del servicio ante fallos, interrupciones o rescisión de contratos (art. 28.8 del Reglamento DORA)

Integración en el marco general de gestión de riesgos TIC: Alinear la gestión del riesgo de terceros con el resto del sistema de control interno, para tener una visión consolidada de la exposición global.

En conjunto, estas prácticas permiten cumplir con los requisitos del Capítulo V del Reglamento DORA y fortalecer la resiliencia operativa digital, asegurando que la dependencia de terceros no comprometa las funciones críticas de la entidad.