Informe sobre el resultado de la autoevaluación sobre la preparación de las entidades con respecto a DORA

Dirección General de Política Estratégica y Asuntos Internacionales

Departamento de Estrategia, Innovación y Finanzas Sostenibles

4 de diciembre de 2024

Índice

1	**Introducción**		**5**
2	**Cuestionario sobre la preparación de DORA**		**6**
3	**Participación de las entidades financieras**		**8**
4	**Gestión de riesgos TIC**		**12**
	4.1	Gobernanza y organización	12
	4.2	Marco de gestión de riesgos TIC	14
	4.3	Políticas y procedimientos	15
	4.4	Identificación, detección, protección, respuesta y recuperación	17
5	**Gestión de incidentes relacionados con las TIC**		**22**
6	**Pruebas de resiliencia operativa digital**		**25**
7	**Gestión del riesgo relacionado con las TIC derivado de terceros**		**27**
8	**Acuerdos de intercambio de información**		**32**
9	**Conclusiones**		**33**
Anexo	**Referencias normativas en distintos ámbitos**		**34**

1 Introducción

En diciembre de 2022 se publicó el Reglamento DORA (DORA o Reglamento) sobre la resiliencia operativa digital, como parte del paquete de finanzas digitales. La entrada en aplicación de este reglamento se producirá el 17 de enero de 2025.

Aunque aún están pendientes de aprobación por la Comisión Europea varios desarrollos normativos de nivel 2 y 3, ya se han publicado las versiones finales de todos sus borradores.

La CNMV ha lanzado un formulario de autoevaluación, que no supone un ejercicio de supervisión, con un doble objetivo:

— Conocer el estado de preparación de las empresas de servicio de inversión y las gestoras con respecto a DORA.

— Incentivar un ejercicio de autoevaluación que permita a las entidades identificar los aspectos que las distancian del cumplimiento del Reglamento y planificar su implementación.

A lo largo de este documento, resaltadas en recuadros, se indican algunas recomendaciones (con el símbolo), expectativas ( ), normativa a destacar ( ) y referencias a materiales de aclaración de carácter más técnico que pueden resultar de ayuda, principalmente, a **entidades de tamaño pequeño y mediano**.

Los datos recogidos en este informe se basan en el análisis de las respuestas de las entidades al cuestionario elaborado por la CNMV. Se trata, por tanto, de un ejercicio de autovaluación realizado por las entidades, cuyas respuestas no han sido verificadas por la CNMV.

El informe contiene recomendaciones al sector, pero en ningún caso debe considerarse que este documento tiene carácter normativo.

2 Cuestionario sobre la preparación de DORA

En función del tamaño de la entidad, se ha adaptado el número de preguntas y el contenido del cuestionario[1].

El cuestionario se ha divido en las siguientes secciones:

— **Sección general** de toma de datos de la entidad y su estado de implementación actual con respecto a DORA.

— **Gestión de riesgos relacionado con las tecnologías de la información y las comunicaciones (TIC).** Esta sección se estructura en los siguientes apartados:

  • Gobernanza y organización.

  • Marco de gestión de riesgos TIC.

  • Políticas y procedimientos.

  • Identificación, detección, protección, respuesta y recuperación.

— **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.**

Para evaluar el grado de madurez, muchas de las preguntas admitían tres respuestas: i) una implementación muy completa de los requisitos de los artículos de DORA, ii) una implementación parcial de estos requisitos y iii) si el Reglamento está pendiente de implementar.

En otro tipo de preguntas, las entidades tenían que seleccionar las opciones que se les aplicaban de entre una lista de elementos (por ejemplo, el contenido en el clausulado de contratos con proveedores, la realización de tipos de pruebas de resiliencia, las medidas de protección, etc.).

1 Así, por ejemplo, a las microempresas no se les aplican algunos requisitos como el apartado 3 del artículo 5, o a las empresas de servicios de inversión pequeñas y no interconectadas se les aplica un marco simplificado de gestión de riegos TIC, definido en el artículo 16, en lugar de los artículos 5 al 15 (véanse los considerandos 42 y 43 de DORA).

Se recomienda a las entidades financieras que revisen los borradores finales RTS e ITS[2] una vez estén aprobados. Las novedades normativas se pueden consultar en la web de la CNMV, en la sección de «Ciberseguridad»[3], y en la los sitios web de las autoridades europeas de supervision (AES[4]).

2 RTS (*Regulatory Technical Standards*): normas técnicas de regulación, ITS (*Implementing Technical Standards*): normas técnicas de ejecución.

3 https://www.cnmv.es/portal/ciberseguridad.aspx

4 https://finance.ec.europa.eu/digital-finance/cyber-resilience_en

3 Participación de las entidades financieras

Los tipos de entidades financieras para las que la CNMV es autoridad competente con arreglo a DORA son las siguientes (artículos 2 y 46 de DORA):

— Empresas de servicios de inversión (las empresas de asesoramiento financiero nacionales [EAFN] no entran dentro de esta definición).

— Las sociedades de gestión.

— Los gestores de fondos de inversión alternativos (salvo los que se indican en el apartado 3 del artículo 2, letra a).

— Los proveedores de servicios de financiación participativa.

— Los proveedores de servicios de criptoactivos.

— Los administradores de índices de referencia cruciales.

— Las infraestructuras de mercados (depositarios centrales de valores, entidades de contrapartida central y centros de negociación).

No obstante, este cuestionario se dirigió únicamente a las empresas de servicio de inversión (ESI), a las gestoras y a los proveedores de servicios de financiación participativa (PSFP). Dichas entidades pudieron enviar sus respuestas **durante los meses de junio y julio de 2024**.

La participación ha sido de un 74 %. En concreto, se han recibido respuestas de **245 entidades**:142 de ESI, 94 de gestoras y 9 de PSFP.

— De las 190 ESI: han respondido 81 sociedades y agencias de valores (SAV) y 61 empresas de asesoramiento financiero (EAF).

— De las 112 gestoras a las que se les aplica DORA, han respondido 89 sociedades gestoras de instituciones de inversión colectiva (SGIIC) y 5 sociedades gestoras de entidades de capital riesgo (SGECR).

Participación de las entidades financieras

CUADRO 1

	ESI	Gestoras	PFP	Total
Número de entidades	190	112	26	328
Participación	142	94	9	245
%	74,74	83,93	34,62	74,70

Fuente: CNMV.

Participación de las entidades de servicios de inversión y las gestoras

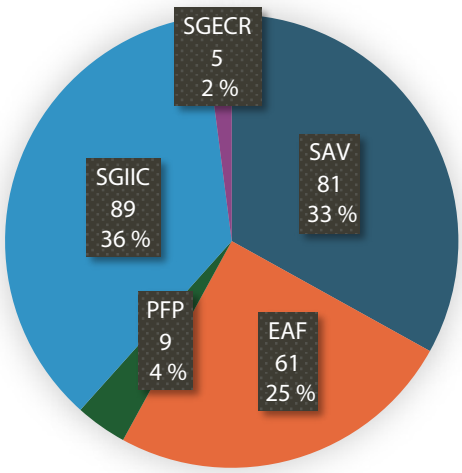
CUADRO 2

	ESI		Gestoras	
	EAF	SAV	SGIIC	SGECR
Número de entidades	89	101	101	11
Participación	61	81	89	5
%	68,54	80,20	88,12	45,45

Fuente: CNMV.

Participación por tipo de entidad

GRÁFICO 1



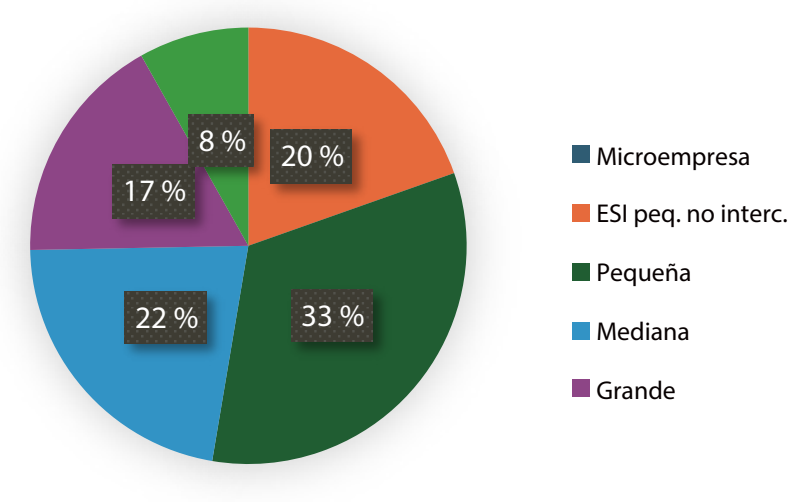
Fuente: CNMV.

Interesa resaltar que 152 gestoras (16 SGIIC y 136 SGECR) no participaron en esta encuesta, puesto que no se les aplica DORA porque gestionan fondos alternativos solamente y no superan los umbrales establecidos en el apartado 2 del artículo 3 de la Directiva 2011/61, relativa a los gestores de fondos de inversión alternativos.

Se recomienda que las **sociedades gestoras de fondos alternativos excluidas** del ámbito de aplicación de DORA apliquen de manera voluntaria el reglamento, si tienen previsto superar a corto o medio plazo los umbrales establecidos en el apartado 2 del artículo 3 de la Directiva 2011/61.

De las entidades que han contestado el cuestionario, si se tiene en cuenta la clasificación por tamaño recogida en el artículo 3 de DORA, solo el 8 % (20) son **grandes empresas**. La mayoría son **pymes**, con un gran número de **microempresas** (20 %, 48 de ellas) y un 33 % (81) se beneficia del **marco simplificado de gestión de riesgos**[5].

Tamaño de las entidades GRÁFICO 2



Fuente: CNMV.

Dado que DORA establece un marco regulador único para todas las entidades financieras, desde los grandes bancos, compañías de seguros e infraestructuras de mercado hasta las pequeñas entidades de asesoramiento financiero, el principio de **proporcionalidad** tiene una gran relevancia en el reglamento y en sus RTS.

En concreto, el artículo 4 del reglamento recoge este principio:

> «1. Las entidades financieras **aplicarán las normas** establecidas en el capítulo II (marco de gestión de riesgos) 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**.
>
> 2. Además, la **aplicación** por parte de las entidades financieras de los capítulos III y IV (notificación de incidentes y pruebas) y el capítulo V (riesgos TIC de terceros), sección I, será **proporcional a su tamaño y perfil de riesgo general, así como a la naturaleza, escala y complejidad de sus servicios, actividades y operaciones**, tal como se establece específicamente en las normas pertinentes de dichos capítulos».

Es decir, en la aplicación de los requerimientos recogidos en los capítulos mencionados, se tendrá en cuenta, además del perfil de riesgo general inherente a su actividad, el tamaño y otros aspectos de la entidad y su operativa.

5 Entre otros, se les aplica el artículo 16 de DORA en lugar de los artículos 5 al 15.

Por otro lado, según el tipo y el tamaño de la entidad, se contemplan distintas exenciones de requisitos (microempresas) o una mayor flexibilidad (como las ESI pequeñas y no interconectadas, a las que se les aplica un régimen simplificado del marco de gestión de riesgo[6]) o la ampliación de requisitos para entidades más críticas (como las entidades de contrapartida central).

Además, como norma general, en DORA se sugiere un enfoque basado en el riesgo; por ejemplo, teniendo en cuenta las funciones esenciales o importantes.

Como cuestión general, se ha preguntado a las entidades sobre el **grado de adaptación respecto a DORA**:

— El 18 % ya había revisado su adecuación y había asignado los recursos necesarios para su cumplimento.

— El 58 % estaba en proceso de revisión y ejecutando algún plan.

— El 24 % tenía previsto realizar el proceso de revisión, pero todavía no lo había hecho. De ellas, un 83 % no pertenece a un grupo de empresas y un 95 % está compuesto por microempresas o pequeñas empresas.

La conclusión es que existe un porcentaje elevado (24 %) de entidades que estaban pendientes de realizar dicha revisión. Además, destaca —como era previsible— que las más preparadas son las entidades de mayor tamaño y las que pertenecen a un grupo, puesto que en general cuentan con más recursos para gestionar estos procesos de revisión de la nueva normativa.

Con carácter previo a la aplicación de DORA, las entidades financieras tendrían que haber realizado un proceso de **análisis de cumplimiento** (o análisis GAP) y disponer de un plan de implementación, con recursos y responsabilidades asignados.

6 Considerandos 42 y 43 de DORA.

4 Gestión de riesgos TIC

El cuestionario contenía una sección relacionada con los artículos 5 al 16 de DORA y los RTS sobre el marco de gestión de riegos TIC y el marco simplificado.

Esta es la sección del cuestionario con más preguntas, al ser la base para que las organizaciones consigan una capacidad adecuada de ciberresiliencia. Las entidades deben incorporar esta gestión dentro de sus procesos empresariales, en la gobernanza y asignación de responsabilidades, en la integración con los demás riesgos de la empresa (principalmente dentro del riesgo operacional), en la estandarización y madurez de sus procesos (con estrategias, políticas y procedimientos) y en la revisión y mejora continua (de la que debe encargarse la función de control o auditoría interna, y con un reporte al órgano de dirección).

Con carácter general, las entidades financieras ya tenían la obligación de llevar a cabo una adecuada gestión de riesgos[7]. Con DORA se exige además una gestión de los riesgos relacionados con las TIC. Esta gestión requiere un tratamiento específico debido, entre otros factores, a la necesidad de protección de la disponibilidad, autenticidad, integridad y confidencialidad de los datos, la complejidad de los sistemas y procesos, la exposición a ciberamenazas, el panorama cambiante, tanto de tecnología como de amenazas, y la elevada dependencia de proveedores terceros.

4.1 Gobernanza y organización

En DORA se resalta la importancia de la gobernanza y la organización de la ciberresiliencia[8], haciendo al órgano de dirección el responsable último de la gestión del riesgo tecnológico de su entidad.

Es fundamental que la gestión de la ciberresiliencia esté bien gobernada y tenga el respaldo de la dirección. De hecho, el Instituto Nacional de Estándares y Tecnología (NIST) incorpora un apartado «Gobernar» —novedad en la versión 2.0 de su marco de ciberseguridad[9]— como la función necesaria para lograr y priorizar las demás funciones: identificación, protección, detección, respuesta y recuperación.

7 Norma 4.ª de la Circular 6/2009 sobre control interno de las SGIIC y norma 6.ª de la Circular 1/2014 sobre organización interna y funciones de control de las ESI.

8 Artículo 5 de DORA y artículo 28 de los RTS sobre el marco simplificado de gestión del riesgo.

9 https://www.nist.gov/cyberframework

En el caso de las ESI y las gestoras españolas, es el **consejo de administración** el órgano con el máximo nivel de decisión de la entidad, responsable de definir, aprobar y supervisar todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC. Si bien la responsabilidad recae siempre en dicho órgano, la gestión operativa puede delegarse en una comisión o similar.

La mayor parte de las entidades encuestadas ya ha implementado de manera muy completa medidas de gobernanza y organización, destacando la aprobación de la política de continuidad (55 % de las entidades), los planes de auditoría interna (45 %) y la asignación de presupuestos (44 %). No obstante, las respuestas muestran que hay elementos básicos que todavía no están del todo implementados. Así, el 29 % de las entidades indicaba que no tenía una **estrategia de resiliencia operativa digital** y el 38 % no había designado aún un **cargo para el seguimiento de los acuerdos con terceros**.

De manera similar, también se percibe un importante margen de mejora en el caso de las entidades a las que se les aplica el marco simplificado de gestión del riesgo, en algunos aspectos fundamentales. En concreto, sobre gobernanza y organización destaca la falta de **informes periódicos al órgano de gobierno** en esta materia (un 69 % no lo encargaba) y la **aprobación y revisión periódica del marco de gestión de riesgos TIC** (un 44 % no lo implementaba). La mayoría de las entidades indicaba que el órgano de gobierno establecía los objetivos de seguridad (69 %), implementaba las políticas y los procesos (68 %) y definía las responsabilidades (64 %).

El órgano de gobierno deberá estar informado periódicamente de los principales riesgos relacionados con las TIC y de la revisión de su marco de gestión para su aprobación.

Uno de los problemas comunes en materia de ciberresiliencia es la falta de comunicación entre los directivos y los responsables de las TIC. En DORA se incluye la necesidad de una formación de los directivos y de unos procesos de comunicación adecuados[10], ya que resulta fundamental para que exista un diálogo fluido con la alta dirección[11].

Puede consultarse el **Código de buen gobierno de la ciberseguridad**[11], elaborado por el Foro Nacional de Ciberseguridad. Este código ofrece recomendaciones de alcance general, organizadas en principios para que pueda ser utilizado por cualquier organización que persiga mantener una adecuada gobernanza de la ciberseguridad.

10 Apartado 4 del artículo 5 y artículo 14 de DORA, respectivamente.

11 http://cnmv.es/DocPortal/Ciberseguridad/CBG_Ciberseguridad.pdf

4.2 Marco de gestión de riesgos TIC

Los artículos 6 y 16 de DORA requieren que las entidades implementen un marco de gestión de riesgos relacionados con las TIC.

Un marco de gestión de riesgos TIC suele incluir las siguientes etapas:

— Identificación de riesgos (activos, amenazas y vulnerabilidades).

— Valoración de riesgos (cálculo y evaluación de los riesgos).

— Tratamiento de riesgos (medidas de salvaguarda o controles de mitigación y cálculo del riesgo residual).

— Monitorización del riesgo (valoración de la efectividad de las medidas y seguimiento del riesgo).

En ciberseguridad hay diferentes marcos de gestión estándar. Cada entidad puede adoptar el que mejor se adapte a su situación, revisando que se adecue a los requisitos de DORA. Como referencia para pymes, cabe destacar los recursos del INICBE[12], el CCN[13] y otras guías como la de ENISA[14] o la de NIST[15].

Según DORA, a las gestoras **no** se les aplica **el marco simplificado** de gestión de riesgos relacionado con las TIC.

El marco simplificado se aplica, en este contexto, a las entidades que sean «**empresas de servicio de inversión pequeñas y no interconectadas**»[16].

Los datos recabados en el cuestionario muestran que el 37 % de las entidades no tiene un **marco de gestión de riesgos TIC** implementado y solo el 22 % lo implementa de una manera muy completa. Un 18 % no ha separado las **funciones de control y gestión**, mientras que un 54 % aplica las tres líneas de defensa (gestión, control y auditoría interna).

No cabe duda de que a las entidades de pequeño tamaño y que no pertenecen a un grupo les resulta más difícil implementar esa segunda línea, por lo que establecen una línea de gestión y otra de control y auditoría interna. La mayor parte de las entidades que tienen un marco de gestión, **lo revisan**, aunque un 45 % no lo hace con la frecuencia debida o con el detalle que se indica en DORA. Un gran número de entidades (43 %) realiza **auditorías periódicas** del marco de gestión llevando un seguimiento de los resultados. El 45 % no ha definido claramente una **estrategia de resiliencia** operativa digital.

12 https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo

13 https://pilar.ccn-cert.cni.es/index.php/analisis-de-riesgos/analisis-de-riesgos-pilar

14 https://www.enisa.europa.eu/publications/archive/RMForSMEs

15 https:/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

16 Según el artículo 12, apartado 1, del Reglamento (UE) 2019/2033 del Parlamento Europeo y del Consejo.

En cuanto a las entidades a las que se les aplica el **marco simplificado**, el 63 % realiza un proceso de **identificación** y valoración de sus riesgos TIC. Sin embargo, el 62 % no ha aprobado los niveles de tolerancia al riesgo, el 63 % no define o no **monitoriza la mitigación** de los riesgos respecto a la tolerancia y el 60 % no **revisa periódicamente la valoración** de riesgos (aunque el 58 % generaba algún tipo de informe periódico sobre la **revisión del marco**).

Todas las entidades financieras deberán **documentar y revisar del marco de gestión** de riesgo relacionado con las TIC[17]. La revisión deberá realizarse al menos una vez al año o periódicamente según el tipo de entidad y cuando se produzcan incidentes graves relacionados con las TIC.

La CNMV podrá solicitar un **informe sobre la revisión**. El contenido y formato de dicho informe está descrito en los RTS sobre gestión de riesgos[18].

4.3 Políticas y procedimientos

En los artículos 5 al 16 de DORA y en los RTS se indican un gran número de políticas y procedimientos que se deben incluir dentro del marco de gestión de riesgos relacionados con las TIC, que abarca, entre otros, la gestión de operaciones, la criptografía, la gestión de las vulnerabilidades y parches, la seguridad de los datos, etc.

En DORA se espera de las entidades un nivel de madurez suficiente para que la gestión de su ciberresiliencia esté soportada con estrategias, políticas y procedimientos definidos[19].

Solo el 23 % de las entidades carece de una política de seguridad formalmente aprobada.

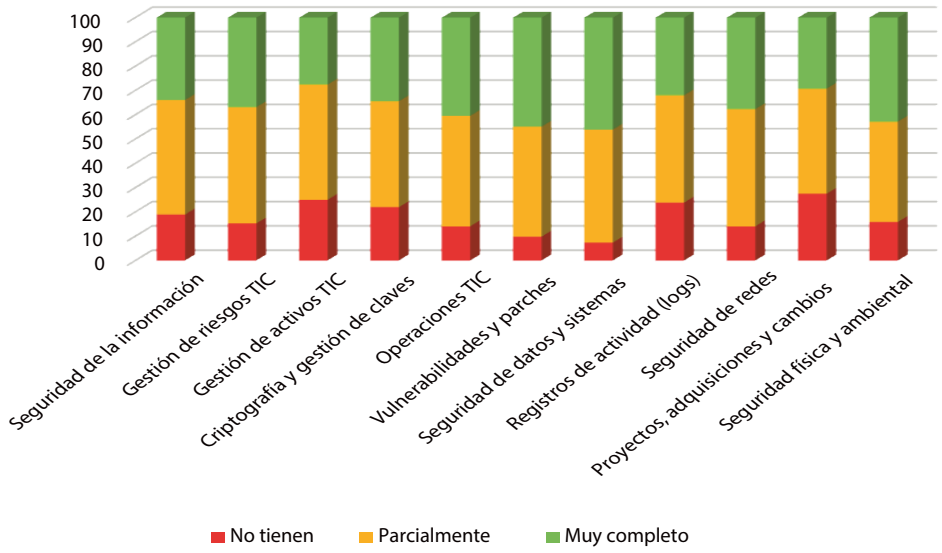
En el cuestionario se preguntó por las diferentes políticas y procedimientos de DORA y los RTS relacionados con el marco de gestión de riesgos. Cabe destacar que el 93 % de las entidades había implementado una política de datos y sistemas; el 90 %, la de gestión de vulnerabilidades y parches de seguridad, y el 86 %, la de operaciones de TIC. Por otro lado, se observaron mayores carencias en las políticas de gestión de proyectos, adquisiciones y cambios (27 %), en las políticas de gestión de activos (25 %) y en la de criptografía y gestión de claves (22 %).

17 Apartado 2 del artículo 6 y apartado 2 del artículo 16.

18 Artículos 27 y 41 de los RTS sobre el marco de gestión de riesgos (RD UE 2024/1772).

19 Al menos el nivel L3 o similar del modelo de madurez (CMM). Disponible en: https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/web/help/html/niveles_de_madurez.html

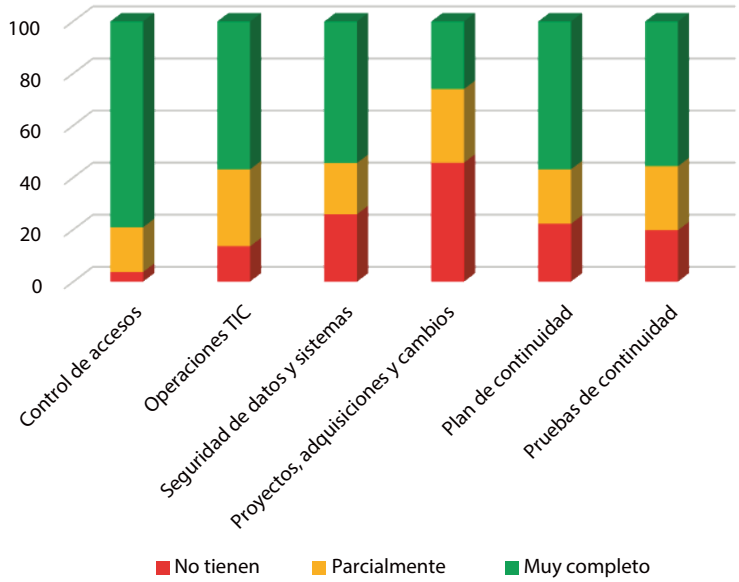
Políticas y procedimientos del marco de gestión de riesgos GRÁFICO 3



Fuente: CNMV.

De las entidades a las que se les aplica el **marco simplificado**, el 76 % tenía implementado un control de accesos robusto; el 49 % gestionaba sus activos TIC durante su ciclo de vida (no solo en el momento de su adquisición); el 26 % implementaba medidas de seguridad básicas sobre sus datos, sistemas y redes; el 78 % tenía implementado un plan de continuidad, y el 80 % hacía pruebas de sus mecanismos de recuperación.

Procedimientos del marco simplificado de gestión de riesgos GRÁFICO 4



Fuente: CNMV.

Se recomienda a las entidades que ya cuenten con políticas de seguridad, continuidad y respaldo, que revisen si estas cumplen con DORA o si deben adaptarlas o implementar políticas y procedimientos adicionales. Deben ser aprobadas por el órgano de dirección y revisadas periódicamente.

4.4 Identificación, detección, protección, respuesta y recuperación

De manera similar a NIST[20], la sección II del capítulo II de DORA (artículos 8 al 14 y 16) se estructura siguiendo las funciones de la gestión del riesgo relacionado con las TIC: identificación, protección y prevención; detección; respuesta y recuperación; aprendizaje, y evolución y comunicación.

i) La fase de **identificación** es fundamental para poder gestionar la ciberresiliencia. Se deben identificar, por un lado, las funciones empresariales y los activos de TIC, clasificarlos y documentarlos con sus interdependencias y, por otro lado, las fuentes de riesgos a las que están expuestos.

Para la **identificación de fuentes de riesgos**, hay catálogos de amenazas disponibles dentro de los estándares de marcos de gestión de riesgos. Algunos ejemplos son el de Pilar/Magerit v3[21] o el de Secure Controls Framework[22].

El 21 % de las entidades indicaba que no tenía documentado un proceso de identificación y clasificación de funciones y activos de TIC, y el 44 % lo realizaba de una manera parcial. En un 14 % de las respuestas no se llevaba a cabo un proceso de identificación de amenazas y vulnerabilidades.

Respecto a cambios importantes en los servicios de TIC, el 86 % reevaluaba los riesgos. De ellos, el 49 % lo hacía de una manera muy completa, incluyendo sistemas heredados (*legacy*).

Si no se realiza una **identificación** adecuada, la entidad merma su capacidad de controlar los riesgos a los que está expuesta, al haber sistemas, activos o amenazas no gestionados[23]. La **clasificación** permitirá poner el foco en los sistemas y activos TIC más importantes para la entidad.

ii) Sobre la **detección y respuesta**, el 88 % tenía implementados sistemas de monitorización y alerta sobre sus servicios; de ellos, el 51 % contaba con mecanismos automatizados de alerta temprana. Sobre la capacidad de respuesta, el 85 % disponía de recursos proactivos de monitorización y el 46 % tenía automatizados los procesos de respuesta.

Se recomienda **automatizar**, en la medida de lo posible y según la capacidad de cada entidad, los procesos de detección y respuesta, para minimizar los tiempos de incidentes (hay medidas que van desde alertas automáticas por correo electrónico o protecciones EDR/XDR hasta productos más avanzados, como SIEM para correlacionar los registros de actividad y SOAR de orquestación de respuestas).

20 https://www.nist.gov/itl/smallbusinesscyber
21 https://pilar.ccn-cert.cni.es/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos
22 https://securecontrolsframework.com/risk-management-model/#threat-catalog
23 https://www.incibe.es/empresas/blog/shadow-it-lo-que-hay-en-la-sombra-de-tu-organizacion

iii) Con base en la gestión de riesgos, cada entidad deberá implementar las **protecciones** adecuadas para limitar o contener el impacto de las amenazas potenciales con el fin de desempeñar sus funciones de negocio con arreglo a sus políticas y procedimientos. Dentro de estas medidas, cabe destacan:

- La protección de la identidad: identidades únicas, políticas de contraseñas robustas, doble factor de autenticación o MFA, gestores de contraseñas, etc.
- La autorización: principio de mínimo privilegio, necesidad de saber y procedimientos de altas, bajas y modificaciones robustos.
- La protección de la superficie de exposición: servicios expuestos a internet o a terceros.
- La protección del puesto de trabajo y otros dispositivos del usuario: antivirus, bastionado, almacenamiento extraíble, cifrado, etc.
- La protección de los datos: su disponibilidad, integridad y confidencialidad.
- La seguridad de las redes y los sistemas: alta disponibilidad, bastionado, confianza cero, VPN, etc.
- El desarrollo seguro de código, separación de entornos y gestión de cambios.
- La protección de la administración de los sistemas: usuarios privilegiados, segmentación de redes, monitorización, gestión de los registros de actividad y alertas, etc.

En la encuesta se ha preguntado por diferentes sistemas de protección. Las entidades tenían un número variado de soluciones, siendo las más comunes: sistemas de antispam, cifrado de las comunicaciones de internet, antivirus, cortafuegos y sistemas de alta disponibilidad.

La gran variedad de productos y soluciones de seguridad que ofrece el mercado puede dificultar la toma de decisiones adecuadas. Además, hay que tener en cuenta que no basta con adquirir un producto si no se configura según las características propias de la entidad. Por ello resulta necesario el análisis de la gestión de los riesgos, **para priorizar y dimensionar adecuadamente las medidas de mitigación** según la capacidad de la entidad. Además, los productos y soluciones implementados se deben **mantener con el tiempo y comprobar su eficacia** en la mitigación. Para asegurar ese trabajo, son muy importantes las funciones responsables del control, de la auditoría interna y de las pruebas de resiliencia. Existen diferentes guías para configurar los productos de manera segura, como las del CCN[24] o las del CIS[25].

24 https://www.ccn-cert.cni.es/es/guias.html
25 https://www.cisecurity.org/cis-benchmarks

Las protecciones de seguridad y resiliencia implementadas por las entidades deben estar debidamente configuradas y mantenidas, con las últimas actualizaciones de seguridad.

iv) Sobre la **recuperación**, en el artículo 11 de DORA se incluyen los planes de continuidad de la actividad en materia de TIC[26], para garantizar la continuidad de las funciones esenciales o importantes de la entidad.

El 81 % de las entidades ya contaba con una política de continuidad de la actividad, y el 86 % lo probaba, aunque el 34 % de manera ocasional. El 77 % realizaba análisis del impacto de negocio (BIA[27]). El 88 % tenía asignada la función de gestión de crisis.

El 93 % implementaba procedimientos y planes de respuesta y recuperación en materia de TIC y el 70 % los auditaba internamente.

Todas las entidades realizaban copias de respaldo: el 67 % empleaba mecanismos de gran robustez y el resto usaba métodos más básicos.

Los **planes de continuidad de la actividad** en materia de TIC deberán cumplir con los niveles y plazos de recuperación previstos, aprobados por el órgano de dirección, que deberán ser acordes con las características de la entidad (tamaño, perfil de riesgo general y naturaleza, escala y complejidad de sus servicios, actividades y operaciones).

v) El **aprendizaje y evolución** también constituye una parte muy importante de la ciberresiliencia en DORA. La rápida evolución de la tecnología presenta nuevas oportunidades de negocio (servicios en la nube, inteligencia artificial [IA], tecnologías 5G, etc.) pero también las ciberamenazas van aumentando (*malware* como servicio, *deepfake* y otros usos de la IA, criptografía cuántica, actores Estado-nación, etc.).

La ciberresiliencia de una entidad debe ir evolucionando y madurando con el tiempo; debe ser un proceso de mejora continua. El órgano de dirección ha de comprender los riesgos tecnológicos que le afectan, los usuarios deben tener una buena formación acerca de las políticas y concienciación en ciberhigiene, y el personal técnico debe seguir los procedimientos y buenas prácticas en materia de ciberresiliencia.

26 https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio
27 https://www.incibe.es/empresas/blog/pasos-seguir-realizar-analisis-impacto-negocio

Para la **identificación de vulnerabilidades, ciberamenazas e incidentes** relacionados con las TIC, referidas en el apartado 1 del artículo 13 de DORA, se recomiendan medidas como:

- Suscripción a los avisos de seguridad del INCIBE o del CCN-CERT u otro organismo similar[28].
- Revisión de las útlimas versiones y actualizaciónes de seguridad (*release notes*) de los principales fabricantes/productos empleados o suscripción a sus boletines.
- Revisión periódica de los informes sobre el panorama de amenzas, como el de ENISA, o de paneles de incidentes[29].
- Colaboración con otras entidades y participación en foros y eventos de ciberseguridad (véase la sección 8 sobre acuerdos de intercambio de información).
- Consulta de otras fuentes como la de Mitre, que documenta las técnicas tácticas que usan los ciberdelincuentes[30], o la de OWASP, con los 10 riesgos de seguridad más importantes en aplicaciones web[31].

DORA no debe suponer un cambio descontrolado en las entidades que, debido a la complejidad de nuevos sistemas o procedimientos, ponga en peligro su operativa por falta de conocimientos o capacidad.

Se recomienda **implementar los cambios de mayor riesgo de manera gradual y controlada**, de acuerdo con la capacidad de cada entidad, priorizando las funciones esenciales e importantes.

Las diferentes pruebas de ciberresiliencia, los mecanismos de control y auditoría, y los sistemas de detección y alerta deben ayudar a actualizar los riesgos relacionados con las TIC de la entidad.

DORA no debe entenderse como un esfuerzo puntual para cumplir con la regulación. Las entidades financieras deben implementar procedimientos para **mantener y desarrollar su capacidad de ciberresiliencia** con el tiempo.

En el caso de las **entidades pequeñas**, que tienen menos recursos para adaptarse a los nuevos requisitos de DORA y **aplicando el principio de proporcionalidad**, aunque no tengan implementadas todas las medidas requeridas de manera completa para cuando sea de aplicación el Reglamento, sí se espera que tengan definido y presupuestado un plan de implementación que contemple este esfuerzo para ir desarrollando dicha capacidad de ciberresiliencia en un plazo razonable.

28 https://www.incibe.es/incibe/suscripciones y https://www.ccn-cert.cni.es/es/seguridad-al-dia.html
29 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends y https://ciras.enisa.europa.eu/
30 https://attack.mitre.org/
31 https://owasp.org/www-project-top-ten/

Aunque es preferible anticiparse a los incidentes, los que ocurran deben servir para mejorar los procesos y medidas de mitigación y para analizar qué controles no han sido eficaces o qué salvaguardas deben reforzarse ante determinadas amenazas.

vi) **Finalmente**, la **comunicación** es otro elemento clave en la gestión de la ciberresiliencia. Las entidades deben contar con un plan de comunicación de crisis, para divulgar de manera responsable los incidentes graves relacionados con las TIC o las vulnerabilidades a quien proceda (personal interno, clientes, contrapartes o público), como se indica en el artículo 14 de DORA.

5 Gestión de incidentes relacionados con las TIC

La gestión de incidentes tiene su ciclo de vida y no empieza en el momento que se detecta un incidente (previamente se deben reunir las herramientas necesarias para la gestión, se han de establecer los criterios de clasificación y alerta, los roles y responsabilidades, etc.). Cada entidad debe estar lo mejor preparada posible, para evitar la improvisación en el momento que ocurra (como ejemplo, puede consultar las guías del INCIBE[32]).

Las preguntas incluidas en esta sección del cuestionario están relacionadas con los artículos 17 al 20 de DORA, los RTS sobre criterios de clasificación de incidentes relacionados con las TIC, las Directrices sobre costes y pérdidas y los RTS e ITS sobre notificación de incidentes importantes.

En esta sección es, en general, en la que se ha visto menos preparadas a las entidades. El 35 % no tenía definida una **política de gestión de incidentes** y en el 36 % de los casos era genérica. El 36 % no implementaba un mecanismo de **clasificación y registro de incidentes**. En el 29 % de las respuestas no se habían designado las **funciones y responsabilidades** o definido los **planes de comunicación**. Un 22 % no había realizado los preparativos necesarios para **notificar a la CNMV** los incidentes graves.

Las entidades financieras del ámbito de la CNMV deberán **comunicarle los incidentes graves relacionados con las TIC** (la notificación inicial, informe(s) intermedio(s) y el final) tal y como se indica en DORA, artículo 19, y sus RTS.

Consulte la siguiente página web[33], dentro de la sección de «Ciberseguridad» del portal de la CNMV, para conocer la manera de notificar los incidentes graves y las ciberamenazas importantes.

Adicionalmente, si el incidente grave relacionado tiene consecuencias para los **intereses financieros de los clientes**, las entidades financieras deberán informarlos y comunicarles todas las medidas que se hayan adoptado[34].

Sobre los **criterios de clasificación** de un incidente, en los RTS se han definido los criterios y los umbrales para clasificar un incidente como grave[35]. Se considera **incidente grave** si cumple con alguna de las siguientes condiciones sobre la esencialidad de los servicios afectados:

32 https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad y https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf

33 http://cnmv.es/DocPortal/Ciberseguridad/Comunicacion_incidentes_es.pdf

34 Apartado 3 del artículo 19 del Reglamento.

35 Reglamento Delegado (UE) 2024/1772 de la Comisión sobre los criterios para la clasificación de los incidentes relacionados con las TIC.

i) Afecta a servicios de TIC que sustenten funciones esenciales o importantes de la entidad.

ii) Afecta a servicios financieros prestados por ellas que requieran autorización o registro o que sean supervisados.

iii) Cuando consiga un acceso efectivo, malintencionado y no autorizado a los sistemas TIC de la entidad.

Además, el incidente debe cumplir alguna de las siguientes condiciones:

i) Cuando el acceso malintencionado (punto iii anterior) pueda dar lugar a pérdidas de datos.

ii) Si se cumplen los umbrales especificados en el artículo 9 de los RTS de, al menos, dos de los siguientes criterios:

   a. Clientes, contrapartes financieras y transacciones afectadas (apartado 1).

   b. Repercusión en la reputación (apartado 2).

   c. Duración del incidente y duración de la interrupción del servicio (apartado 3).

   d. Extensión geográfica (apartado 4).

   e. Pérdida de datos (apartado 5).

   f. Consecuencias económicas (apartado 6).

iii) Si en el plazo de seis meses ocurre más de un incidente no grave y cumplen las siguientes condiciones:

   a. La entidad financiera no es una microempresa ni una ESI pequeña no interconectada.

   b. Los incidentes tienen la misma causa subyacente.

   c. A nivel colectivo, los incidentes cumplen con los requisitos de las condiciones previas.

Hay que tener en cuenta que, en la resiliencia operativa digital en general y en los incidentes en particular, no solo se tratan los ciberataques (aunque estos representen una gran amenaza de gran impacto). Además, se tratan los fallos no malintencionados, como los fallos de sistemas (fallos de *hardware* o de *software*), los errores humanos al ejecutar procesos, etc.

Los **plazos previstos**, tal y como se contempla en los RTS e ITS sobre la notificación de incidentes (artículo 6 de los RTS[36]) son los siguientes:

— **Notificación inicial:** hasta las 4 horas de clasificarlo como grave o a las 24 horas desde su conocimiento.

— **Informe intermedio:** hasta 72 horas desde la notificación inicial (y cuando hay actualizaciones pertinentes del informe y una actualización cuando se recupera la actividad normal).

— **Informe final:** hasta un mes desde la última actualización del informe intermedio.

Además de la notificación de los incidentes graves a la CNMV, las entidades podrán notificar con **carácter voluntario** las ciberamenazas que consideren pertinentes para el sistema financiero, los usuarios del servicio o los clientes.

Cuando una entidad sufre un incidente grave se produce una situación complicada que genera mucho estrés. Es fundamental la preparación previa para que se recupere a la mayor brevedad. En este sentido, se recomienda que la entidad implemente los procedimientos para clasificarlos y poder realizar la **notificación a la CNMV en los plazos establecidos** incluyendo todos los datos requeridos.

También se recomienda implementar procedimientos relacionados con el **plan de comunicación a los clientes**, que incluya responsabilidades, criterios para comunicar, plantillas de notificación, canales a emplear, etc.

Las autoridades competentes, a su vez, difundirán estos incidentes a la autoridad europea de supervisión y a otras autoridades pertinentes (como los CSIRT o puntos de contacto únicos de la NIS[37]). Con toda la información recibida y diseminada, las autoridades podrán recopilar mucha inteligencia sobre amenazas para dar mejor respuesta frente a incidentes y beneficiar a las demás entidades financieras y a otras autoridades con el fin de lograr una mejor defensa colectiva.

36 Con excepciones si el incidente ocurre en fin de semana o la entidad tiene problemas para notificar, aunque debe informar a la autoridad de ello.

37 Apartado 6 del artículo 19 de DORA.

6 Pruebas de resiliencia operativa digital

Las entidades deben implementar políticas para probar tanto los **sistemas de TIC** (por ejemplo, vulnerabilidades) como las **personas** que los usan (por ejemplo, campañas de *phishing* o simulación de crisis) y sus **procesos** (por ejemplo, validación de parámetros, control de errores, monitorización, etc.). Hay que probar que los sistemas funcionan de la manera que se espera, que las medidas de mitigación son eficaces y que los procesos de cambio no causen incidentes.

Cada entidad financiera debe realizar las pruebas periódicas de resiliencia operativa digital que considere adecuadas según sus características (tamaño, perfil de riesgo general y naturaleza, escala y complejidad de sus servicios, actividades y operaciones) para lograr un nivel elevado de resiliencia operativa digital, incluyendo **pruebas de los planes de continuidad**.

Las ESI pequeñas no interconectadas establecerán un **plan de pruebas de seguridad** de las TIC (artículo 36 de los RTS del marco simplificado de gestión de riesgos).

Las demás entidades que no sean microempresas deberán establecer y mantener un **programa de pruebas** (artículo 24 de DORA).

Las microempresas realizarán pruebas de una manera más flexible (apartado 3 del artículo 25 de DORA).

El cuestionario ha incluido preguntas relacionadas con los artículos 24 y 25 de DORA. No se han tenido en cuenta los artículos 26 y 27, ya que tratan de pruebas avanzadas de penetración basadas en amenazas, para entidades de gran madurez fuera del alcance de este documento, que está dirigido a entidades de menor tamaño.

Los datos recabados muestran que solo un 34 % tenía implementado un plan de pruebas sólido, esto es, con una periodicidad determinada y haciendo un seguimiento de las deficiencias encontradas. En el 43 % de las entidades, aunque contaban con un plan de pruebas, dichas pruebas no tenían una periodicidad establecida o luego no se hacía un seguimiento formal del resultado. El 23 % de las entidades no tenía un plan de pruebas definido.

En el cuestionario se ha preguntado por algunos tipos de pruebas que realizaban las entidades en distintos ámbitos. Destacan las pruebas de restauración de datos (84 %), de restauración de sistemas (72 %), ambientales (60 %), de rendimiento (53 %) y de penetración (52 %). Solo un 26 % realiza simulaciones de crisis[38].

38 https://www.incibe.es/empresas/formacion/juego-rol-pyme-seguridad

En DORA se identifican diferentes pruebas de resiliencia[39]:

— Evaluaciones y exploraciones de vulnerabilidad.

— Análisis del código abierto.

— Evaluaciones de la seguridad de la red.

— Análisis de carencias.

— Revisiones de seguridad física.

— Cuestionarios y soluciones de *software* de exploración.

— Revisiones del código fuente cuando sea posible.

— Pruebas basadas en escenarios.

— Pruebas de compatibilidad.

— Pruebas de rendimiento.

— Pruebas de extremo a extremo.

 Es primordial analizar y hacer un **seguimiento del resultado** de las pruebas de resiliencia operativa digital, para incorporarlo en la gestión de riesgos relacionados con las TIC de la entidad.

39 Considerando 56 de DORA.

7 Gestión del riesgo relacionado con las TIC derivado de terceros

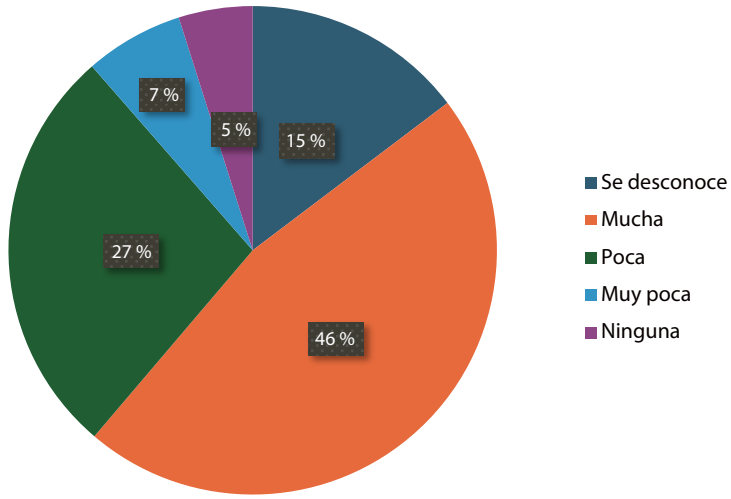
La definición de servicios de TIC es muy amplia, abarca los servicios digitales y de datos prestados a través de sistemas de TIC a uno o varios usuarios internos o externos de forma continua, al igual que es amplia la variedad de proveedores terceros de servicios de TIC que abarca DORA[40].

Se han incluido en el cuestionario preguntas sobre los artículos 28 al 30 de DORA, RTS sobre subcontratación, RTS sobre la política sobre acuerdos con proveedores de servicios de TIC e ITS sobre el registro de proveedores.

Solo el 31 % de las entidades tenía una **estrategia de gestión de riesgos** de terceros implementada. Por otro lado, el 33 % no mantenía un **registro de los contratos** para gestionar los riesgos tecnológicos asociados y únicamente el 23 % llevaba un registro de información muy completo. **Antes de realizar un contrato**, solo el 20 % realizaba un proceso de diligencia debida, mientras que el 35 % no disponía de procedimientos.

Las entidades financieras, por la naturaleza de sus funciones, tienen una gran dependencia, en general, de proveedores de diferentes servicios. Esto se ha visto en las respuestas al cuestionario, que muestran que en el 46 % de los casos dependían de proveedores que no son fácilmente sustituibles o cuyo cambio sería muy costoso. En el 34 % de los casos podrían cambiar de proveedor con un coste estimado asumible (de ellos, el 7 % con muy poca dependencia). Es relevante destacar que un 15 % desconocía el grado de dependencia de sus proveedores.

Dependencia de proveedores de servicios de TIC GRÁFICO 5



Fuente: CNMV.

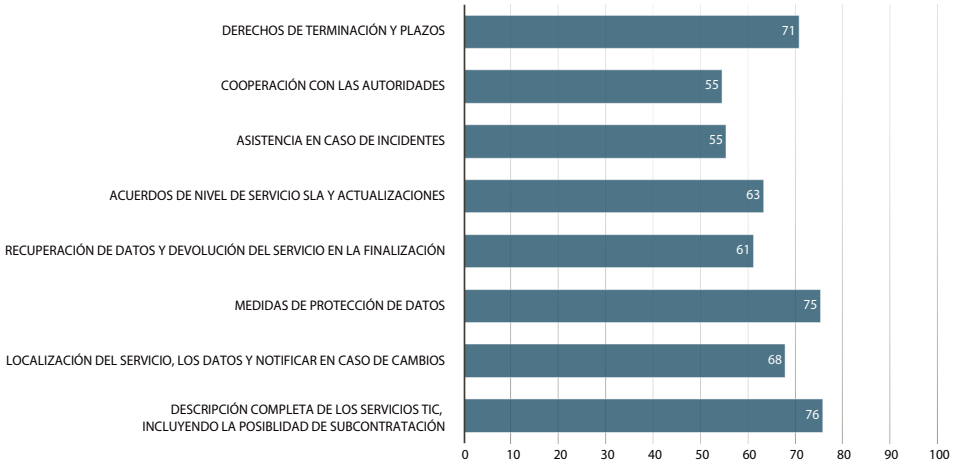
40 Considerandos 35 y 63 de DORA.

En diciembre de 2020 se aprobaron las **Directrices de ESMA sobre la externalización de servicios a proveedores de servicios en la nube**[41]. Estas guías tienen por objeto servir de referencia a las entidades para gestionar la contratación de estos servicios y a las autoridades para su integración dentro del marco supervisor.

Estas directrices se están revisando de forma que sean coherentes con DORA.

A continuación, se indica el porcentaje de entidades que ha identificado, en general, si el clausulado de sus contratos con proveedores de servicios de TIC[42] contenía los siguientes elementos:

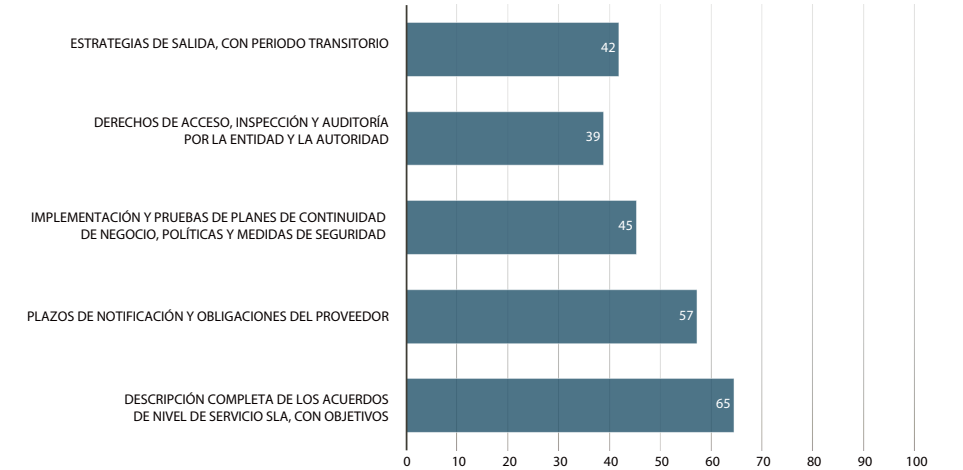
Cláusulas en contratos con proveedores de servicios de TIC GRÁFICO 6



Fuente: CNMV.

El porcentaje que contenía cláusulas más específicas en contratos con proveedores que soportan funciones esenciales o importantes de la entidad[43] es el siguiente:

Cláusulas en contratos con proveedores de servicios de TIC que soportan funciones esenciales o importantes GRÁFICO 7



Fuente: CNMV.

41 https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_es.pdf
42 Apartado 2 del artículo 30 de DORA.
43 Apartado 3 del artículo 30 de DORA.

Se puede observar que, en el primer bloque, lo que menos se cumple es la cooperación con las autoridades y la asistencia en caso de incidentes. En el segundo bloque, el menor grado de cumplimiento está en los derechos de acceso, inspección y auditoría.

Las preguntas relacionadas con **funciones de negocio externalizadas** mostraron que las más comunes son la de control interno (67 %), los servicios y plataformas de intermediarios financieros y contratación de operaciones (50 %) y la seguridad de la información, gestión documental y repositorios de negocio (47 %).

Sobre **servicios digitales y de datos de proveedores** que soportan funciones esenciales o importantes, además de líneas de internet (88 %), destacan los servicios de datos (80 %), de comunicaciones y redes (68 %) y de seguridad TIC (64 %). Para las demás clases de servicios (IaaS, SaaS, de *hardware*, de alojamiento de infraestructura, de gestión de operaciones de TIC, etc.), los datos muestran que más de un 40 % de entidades los usaba.

Las **entidades financieras** que tengan acuerdos contractuales en vigor para utilizar servicios de TIC en el funcionamiento de sus operaciones comerciales serán, en todo momento, **plenamente responsables** del cumplimiento y la observancia de todas las obligaciones de DORA y del derecho aplicable en materia de servicios financieros[44].

Como en otros procesos, la gestión del riesgo derivado de terceros también tiene su ciclo de vida. Comprende las siguientes etapas, que deben estar debidamente documentadas en las políticas de la entidad, para sus servicios esenciales o importantes:

— La valoración previa de los riesgos.

— La debida diligencia.

— La contratación del acuerdo.

— La monitorización del servicio.

— La finalización del servicio.

Se recomienda que las entidades vayan preparando el **registro de proveedores** de servicios de TIC, con la información detallada en los ITS sobre el registro de proveedores[45].

Todas las entidades financieras deberán tener un código LEI[46] (*Legal Entity Identifier*) para su identificación[47] (aunque a los proveedores europeos se les puede exigir otro código de identificación cuando se aprueben los ITS sobre dicho registro).

44 Letra a), apartado 1 del artículo 28 de DORA. Aunque la letra b) añade el principio de proporcionalidad.

45 https://www.esma.europa.eu/press-news/esma-news/esas-announce-timeline-collect-information-designation-critical-ict-third

46 https://cnmv.es/docportal/mifidii_mifir/codigolei.pdf

47 En la fecha de redacción de este documento, en el caso de los proveedores estaba pendiente de definirse su identificador, LEI o EUID. Véase el anexo de los ITS. Disponible en: https://www.esma.europa.eu/press-news/esma-news/esas-respond-european-commissions-rejection-technical-standards-registers

La gestión del riesgo tecnológico derivado de terceros presenta varios retos, entre otros:

— La propia identificación de proveedores de servicios de TIC (siendo una definición muy amplia).

— La inclusión del clausulado necesario y la renegociación en caso de estar incompleto.

— La obtención de la información necesaria para mantener los registros y otros requisitos (cadena de proveedores relevante, monitorización, etc.).

— Muchos proveedores son entidades muy grandes, poco dispuestas a adaptarse a los requisitos de las entidades pequeñas.

Los **proveedores intragrupo** de servicios de TIC están sujetos al mismo marco normativo, aunque al tener mayor nivel de control, se debe tener en cuenta en la evaluación global de riesgos[48].

DORA persigue que la dependencia de terceros se realice de una manera controlada, en condiciones que garanticen una adecuada ciberresiliencia de la entidad, evitando cláusulas abusivas con pocas garantías en la calidad del servicio, el cese no ordenado de la actividad del proveedor o la falta de transparencia en sus procedimientos de resiliencia, además de disponer de una valoración de proveedores alternativos.

DORA permitiría a las entidades más pequeñas acceder más fácilmente a un clausulado que las ayude a gestionar el riesgo de los proveedores de TIC, puesto que es esperable que se cree un marco común en el que las entidades financieras más grandes y, por supuesto, las autoridades incentiven a los proveedores para que lo ofrezcan. Se espera conseguir una mayor **armonización y convergencia** de criterios (con los documentos de preguntas y respuestas que se vayan publicando) y que se normalice la inclusión de adendas financieras en los contratos y las renegociaciones de estos.

Igualmente, el sector se beneficiaría de la **supervisión**, a nivel europeo, de los proveedores que se designen como esenciales y de la capacidad de las autoridades nacionales de supervisión de los proveedores nacionales más relevantes.

Para los contratos de servicios de TIC actuales, especialmente los que soporten funciones esenciales o importantes, se espera una **revisión del clausulado** para conformarlos con los requisitos del Reglamento[49]. Aplicando la proporcionalidad, en los casos en los que no sea factible una renegociación de los acuerdos ni el cambio del proveedor, la entidad deberá tener en cuenta dichos riesgos, cuando deba renovar los contratos.

48 Considerando 31 de DORA.

49 Considerando 69 del Reglamento.

Las autoridades europeas de supervisión —la Autoridad Europea de Valores y Mercados (ESMA), la Autoridad Bancaria Europea (EBA) y la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA)— han organizado en 2024 un simulacro sobre el registro de proveedores, realizando controles de calidad de los datos aportados por las entidades que han decidido participar[50]. Los aspectos más relevantes de esta actuación se han condensado en el documento de preguntas más frecuentes (FAQ) publicado en sus páginas web.

Este registro de proveedores, además de servir a las autoridades para supervisar la exposición de las entidades a determinados riesgos (como la concentración de proveedores en el sector), se usará también para identificar y designar a los proveedores esenciales que serán supervisados por las AES de manera conjunta.

Informe sobre el resultado de la autoevaluación sobre la preparación de las entidades con respecto a DORA

Las entidades financieras comunicarán, al menos una vez al año, a las autoridades competentes **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.

Las entidades financieras informarán oportunamente a la autoridad competente **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[51].

50 https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

51 Apartado 3 del artículo 28 de DORA.

8 Acuerdos de intercambio de información

Al igual que los ciberdelincuentes cada vez actúan de una manera más organizada (con foros de venta y compartición de *malware*, venta de credenciales robadas, hacktivismo, etc.), las entidades financieras deben reforzar la colaboración entre ellas para conocer mejor el panorama de amenazas y compartir los mecanismos de ciberresiliencia, a nivel estratégico, táctico y operativo[52].

Para analizar esta cuestión, relacionada con el artículo 45 de DORA, se han incluido algunas preguntas en el cuestionario.

De las respuestas recibidas, menos de un 20 % de las entidades tenía colaboraciones con la industria (fabricantes y consultoras), con otras entidades financieras (destacando entidades de su propio grupo bancario, asociaciones sectoriales como Inverco o grupos de colaboración como FS-ISAC y FIRST[53]) o con agencias de tipo gubernamental (destacando el INCIBE[54] y el CCN-CERT[55]).

Las entidades **financieras notificarán a las autoridades competentes** su participación en los acuerdos de intercambio de información con otras entidades financieras, conforme a las condiciones referidas en el apartado 1 del artículo 45 de DORA, en el momento en que se valide su incorporación a ellos o, en su caso, el cese de su participación, una vez que se haga efectivo[56].

52 Considerando 34 de DORA.

53 https://www.fsisac.com/ y https://www.first.org/

54 https://www.incibe.es/empresas/blog/que-es-el-reglamento-dora y https://www.incibe.es/empresas

55 https://www.ccn-cert.cni.es/es/

56 Apartado 3 del artículo 45 de DORA.

9 Conclusiones

El lanzamiento del cuestionario de autoevaluación ha permitido concienciar a las entidades financieras sobre los principales requisitos de DORA y ha servido para conocer el estado actual de preparación de las entidades antes de la entrada en vigor del Reglamento.

Adicionalmente, en el proceso de recepción de las respuestas, la CNMV ha estado ayudando al sector respondiendo a sus cuestiones sobre aquellos aspectos en los que más desconocimiento había (se han atendido numerosas consultas sobre la normativa en el buzón de ciberseguridad[57]).

Como conclusiones generales, una vez analizadas en detalle las respuestas de las entidades, se ha observado que, en general, tienen buenas medidas de gobernanza, de ciberseguridad y de continuidad de negocio, aunque faltan en numerosos casos la revisión periódica o el seguimiento de dichas revisiones.

No obstante, se han detectado más carencias en la gestión de incidentes, en la gestión de pruebas y en la gestión del riesgo de proveedores de servicios de TIC. Las entidades de menor tamaño que no pertenecen a un grupo son las que están peor preparadas.

Por lo tanto, se puede concluir que las entidades financieras tienen el reto de adecuarse al nuevo Reglamento y la oportunidad de mejorar su capacidad de resiliencia. En concreto, deberán analizar cómo implementar la regulación en su organización, de manera proporcional a su tamaño, perfil de riesgo y complejidad.

La CNMV colaborará con el sector para que esta implementación se haga de manera eficiente pero también realizará un seguimiento que le permita valorar si se han implementado las medidas de manera adecuada.

57 https://www.cnmv.es/portal/Ciberseguridad.aspx

Anexo Referencias normativas en distintos ámbitos

Las siguientes normas se referenciarán a lo largo de este anexo (situación en la fecha de redacción de este documento):

ID	Norma
DORA	Reglamento de Resiliencia Operativa Digital
RTS1	Reglamento Delegado (UE) 2024/1772 de la Comisión sobre los criterios para la clasificación de los incidentes relacionados con las TIC
RTS2	Reglamento Delegado (UE) 2024/1773 de la Comisión sobre la política sobre acuerdos con proveedores de servicios de TIC
RTS3	Reglamento Delegado (UE) 2024/1774 de la Comisión sobre el marco de gestión de riesgos TIC y el marco simplificado de gestión de riesgos TIC
RTS4	Borrador final RTS sobre los elementos en las pruebas avanzadas de penetración
RTS5	Borrador final RTS e ITS sobre la notificación de incidentes
RTS6	Borrador final RTS sobre armonización de las condiciones para llevar a cabo la supervisión de proveedores esenciales
RTS7	Borrador final RTS sobre la composición de los equipos conjuntos de supervisión de proveedores esenciales
RTS8	Borrador final RTS sobre subcontratación
ITS1	Borrador final ITS sobre el registro de proveedores (rechazado por la Comisión Europea, sujeto a cambios)
GL1	Borrador final Directrices sobre la estimación agregada anual sobre costes y pérdidas causadas por incidentes TIC graves
GL2	Borrador final Directrices para la cooperación en la supervisión e intercambio de información entre las AES y las autoridades competentes

Se incluyen a continuación las referencias a los artículos de las normas más relevantes que regulan los siguientes aspectos:

a) Funciones y responsabilidades

	Ref.
Órgano de dirección (consejo de administración)	DORA 5 DORA 13.5 DORA 17.3.e) DORA 28.2 RTS2 3.1 RTS3 2.2.b) RTS3 15.5 RTS3 25.5 RTS3 27.2.b) RTS3 28.2 RTS3 29.2.a) RTS3 40.3 RTS3 41.2.b)
Cargo para el seguimiento de los acuerdos celebrados con proveedores terceros de servicios de TIC (o miembros de la alta dirección)	DORA 5.3
Función de gestión del riesgo relacionado con las TIC	DORA 6.4
Función de control	DORA 6.4
Función de auditoría interna	DORA 6.4 DORA 6.6
Función de gestión de crisis	DORA 11.7
Función de portavoz ante el público y los medios de comunicación	DORA 14.3

b) Estrategias

	Ref.
Estrategia de resiliencia operativa digital	DORA 6.8 DORA 13.4
Estrategia global multiproveedor (opcional)	DORA 6.9
Estrategia de comunicación sobre incidentes relacionados con las TIC	DORA 14.3
Estrategia relativa al riesgo relacionado con las TIC derivado de terceros	DORA 28.3

c) Políticas y procedimientos

	Ref.
Política de seguridad de la información	DORA 9.4.a) RTS3 29
Política global de continuidad de la actividad en materia de TIC (o parte integrante de la política global de continuidad de la actividad)	DORA 11.1, 2, 5 y 6 RTS 3 24
Políticas y procedimientos de respaldo y procedimientos y métodos de restablecimiento y recuperación	DORA 12
Políticas de comunicación	DORA 14.2
Políticas y procedimientos de seguimiento de los problemas descubiertos durante la realización de las pruebas	DORA 24.5
Política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC	DORA 28.2 RTS2 RTS8
Política y procedimiento de gestión de activos de TIC	RTS3 4 y 5
Política de cifrado y controles criptográficos	RTS3 6
Política de gestión de claves criptográficas	RTS3 7
Políticas y procedimientos relacionados con las operaciones de TIC	RTS3 8
Procedimientos de gestión de la capacidad y el rendimiento	RTS3 9
Procedimientos de gestión de vulnerabilidades y parches	RTS3 10
Procedimiento de seguridad de los datos y sistemas	RTS3 11
Procedimientos de registro	RTS3 12
Políticas y procedimientos en materia de gestión de la seguridad de las redes	RTS3 13
Políticas y procedimientos para proteger la información en tránsito	RTS3 14
Política de gestión de proyectos de TIC	RTS3 15 RTS3 38
Política que regule la adquisición, el desarrollo y el mantenimiento de sistemas de TIC	RTS3 16 RTS3 37
Procedimientos de gestión de cambios en las TIC	RTS3 17 RTS3 38
Política de seguridad física y del entorno	RTS3 18
Política de recursos humanos	RTS3 19
Políticas y procedimientos de gestión de la identidad	RTS3 20
Política de control de acceso y procedimiento de gestión de cuentas	RTS3 21
Política de gestión de incidentes relacionados con las TIC	RTS3 22
Política y procedimiento de gestión de activos de TIC	RTS 3 23.5
Procedimientos para controlar el acceso lógico y físico	RTS3 33
Procedimientos de copia de seguridad y restauración	RTS3 39 y 40

d) Planes

	Ref.
Plan de respuesta y recuperación	DORA 5.e) DORA 11.6 DORA 11.8 DORA 13.3 DORA 15.f) RTS3 26
Plan de auditoría	DORA 5.f) DORA 6.6 RTS2 3.8 RTS3 28
Plan de continuidad de la actividad	DORA 11.6 DORA 11.7 DORA 11.8 DORA 13.3 DORA 15.e DORA 16.1.f) y 16.1.g) RTS3 25 RTS3 39
Plan de comunicación de crisis	DORA 11.6.b) DORA 14.1
Plan de pruebas	DORA 11.6 RTS3 36
Plan de salida y de transición de servicios de TIC de proveedores	DORA 28.8

e) Informes y registros

	Ref.
Informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC	DORA 6.5 RTS3 27
Informe sobre la revisión del marco simplificado de gestión del riesgo relacionado con las TIC	DORA 16.2 RTS3 41
Informe sobre incidentes graves relacionados con las TIC	DORA 17.3.e) DORA 19.4 RTS5
Informe sobre la estimación de los costes y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC	DORA 11.10 GL1
Registro de información de proveedores de servicios de TIC	DORA 28.3 ITS1
Registro de activos de TIC	RTS3 4.2.b)
Registro de todos los certificados y dispositivos de almacenamiento de certificados	RTS 3 7.4
Registro de vulnerabilidades detectadas y del seguimiento de su resolución	RTS3 10.2.h)
Registros de actividad, control de acceso e identidad	RTS3 12 RTS3 20 RTS 3.21

f) Revisiones periódicas

	Ref.
Aplicación de la **política de continuidad de la actividad** en materia de TIC y de los **planes de respuesta y recuperación** en materia de TIC	DORA 5.2.e) DORA 11.6
Planes de auditoría internos de TIC y las auditorías de TIC de la entidad financiera, así como sus modificaciones significativas	DORA 5.2.f)
Política sobre los acuerdos relativos al uso de servicios de TIC prestados por proveedores terceros de servicios de TIC	DORA 5.2.h)
Políticas, procedimientos, protocolos y herramientas en **materia de seguridad** de las TIC	RTS3 2.2.j)

g) Revisiones anuales

(En algunos casos, periódicamente para microempresas)	Ref.
Presupuesto necesario para satisfacer las necesidades de resiliencia operativa digital	DORA 5.2.g) RTS3 28.2.e)
Marco de gestión del riesgo relacionado con las TIC	DORA 6.5 DORA 16.2 RTS3 31.2
Idoneidad de la **clasificación y la documentación** de todas las funciones, cometidos y responsabilidades empresariales sustentados por las TIC, los activos de información y activos de TIC que sustenten dichas funciones, y sus cometidos y dependencias en relación con el riesgo relacionado con las TIC	DORA 8.1
Escenarios de riesgo relacionado con las TIC que las afecten	DORA 8.2
Evaluación específica del **riesgo** relacionado con las TIC en todos los **sistemas de TIC heredados**	DORA 8.7
Someter a **prueba 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	DORA 11.6.a)
Informar al órgano de dirección de los **hallazgos** a los que se refiere el apartado 3 (enseñanzas derivadas de las pruebas y de los incidentes reales relacionados con las TIC) y formular recomendaciones	DORA 13.5
Garantizar que se efectúen las **pruebas apropiadas** de todos los sistemas y aplicaciones de TIC que sustenten funciones esenciales o importantes	DORA 24.6
Comunicar a las autoridades competentes 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	DORA 28.3
Riesgos residuales relacionados con las TIC aceptados	RTS3 3.d).iv
Arquitectura de las redes y del diseño de la seguridad de las redes	RTS3 13.i)
Derechos de acceso (cada seis meses para los sistemas de TIC que sustenten funciones esenciales o importantes)	RTS 21.e).iv
Pruebas de procedimientos de **copia de seguridad y restauración**	RTS3 40
Política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC	RTS2 3.1

h) Obligaciones con la CNMV

	Ref.
Proporcionar, si lo solicita, información completa y actualizada sobre el **riesgo relacionado con las TIC** y sobre su **marco de gestión** de dicho riesgo	DORA 6.3
Presentar, si lo solicita, un informe sobre la **revisión del marco de gestión** del riesgo relacionado con las TIC	DORA 6.5 DORA 16.2
Los depositarios centrales de valores facilitarán copias de los **resultados de las pruebas de continuidad de la actividad** en materia de TIC o de ejercicios similares	DORA 11.9
(Cuando no sean microempresas). Informar, si lo solicita, una **estimación de los costes y pérdidas anuales agregados** causados por incidentes graves relacionados con las TIC	DORA 11.10 GL1
Notificar los **incidentes graves** relacionados con las TIC de conformidad con el apartado 4 del presente artículo (notificaciones iniciales, informes intermedios y finales)	DORA 19.1 DORA 19.4 RTS5
Notificar, de manera voluntaria, **ciberamenazas importantes** cuando consideren que la amenaza es pertinente para el sistema financiero, los usuarios del servicio o los clientes	DORA 19.2 RTS5
Comunicar, al menos una vez al año, la 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	DORA 28.3
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	DORA 28.3
Poner a disposición, cuando se solicite, el **registro completo de información** (de proveedores de servicios de TIC)	DORA 28.3 ITS1
Notificar su **participación en los acuerdos de intercambio de información** a los que se refiere el apartado 1 en el momento en que se valide su incorporación a ellos o, en su caso, el cese de su participación, una vez que se haga efectivo	DORA 45.3
Si va a externalizar la obligación de notificación de incidentes graves, según se contempla en el apartado 5 del artículo 19 de DORA	RTS5 6

i) Exenciones a microempresas o ESI pequeñas no interconectadas

No están obligadas a:	Ref.
Crear un cargo o miembro de la alta dirección para el seguimiento de los acuerdos celebrados con proveedores terceros	DORA 5.3
Asignar la responsabilidad de la gestión y supervisión del riesgo relacionado con las TIC a una función de control	DORA 6.4
Documentar y revisar al menos una vez al año el marco de gestión del riesgo relacionado con las TIC (pero sí periódicamente)	DORA 6.5
Someter a auditoría interna periódicamente el marco de gestión del riesgo relacionado con las TIC	DORA 6.6
Llevar a cabo evaluaciones exhaustivas tras cambios importantes en los procesos y las infraestructuras de su red y sistemas de información	DORA 8.3
Realizar periódicamente análisis de riesgos sobre los sistemas de TIC heredados	DORA 8.7
Someter a auditorías internas independientes la ejecución de los planes de respuesta y recuperación en materia de TIC	DORA 11.3
Disponer de una función de gestión de crisis	DORA 11.7
Ampliar las pruebas sobre los planes de continuidad de la actividad y de respuesta y recuperación para reflejar los escenarios de conmutación entre la infraestructura primaria de TIC y las instalaciones redundantes	DORA 11.6
Comunicar a las autoridades competentes que lo soliciten una estimación de los costes y pérdidas anuales agregados provocados por incidentes graves relacionados con las TIC	DORA 11.10
Mantener capacidades de TIC redundantes	DORA 12.4
Comunicar a las autoridades nacionales competentes los cambios ejecutados a raíz de revisiones realizadas tras incidentes relacionados con las TIC	DORA 13.2
Hacer un seguimiento continuo de los avances tecnológicos pertinentes	DORA 13.7
Establecer un programa completo de pruebas de resiliencia operativa digital como parte integrante del marco de gestión del riesgo relacionado con las TIC	DORA 24 DORA 25.1
Adoptar y revisar periódicamente una estrategia relativa al riesgo relacionado con las TIC derivado de terceros	DORA 28.2
Realizar pruebas avanzadas de herramientas, sistemas y procesos de TIC sobre la base de pruebas de penetración basadas en amenazas	DORA 26.1
Evaluar si los incidentes recurrentes se consideran un incidente grave	RTS1 8.2

Concesiones adicionales a las microempresas:	Ref.
Se debe obligar a las microempresas a que evalúen la necesidad de mantener sus capacidades de TIC redundantes únicamente sobre la base de su perfil de riesgo	DORA 12.4
(En los programas de pruebas de resiliencia operativa digital). A la hora de considerar el tipo y la frecuencia de las pruebas que han de realizarse, deben buscar un equilibrio adecuado entre el objetivo de mantener una elevada resiliencia operativa digital, los recursos disponibles y su perfil de riesgo general	DORA 25.3
Podrán acordar con el proveedor tercero de servicios de TIC la delegación de los derechos de acceso, inspección y auditoría de la entidad financiera en un tercero independiente, que nombrará el proveedor tercero de servicios de TIC	DORA 30.3