CIBERSEGURIDAD Y RESILIENCIA OPERACIONAL: EL REGLAMENTO DORA

Celedonio Villamayor Pozo

20 de diciembre de 2022

INDICE

1. Introducción

Introducción

El sector financiero en general, y el asegurador en particular, se encuentra inmerso en un proceso de transformación digital, que ha provocado un aumento de la complejidad operativa y de la exposición a nuevos riesgos.

Estas nuevas amenazas afectan a las entidades aseguradoras desde la óptica financiera e influyen en su estabilidad operativa, debido a la multitud y heterogeneidad de los potenciales eventos, de su impredecibilidad y gravedad, que pueden a poner en riesgo la supervivencia de una entidad.

La Unión Europea ha decidido fortalecer a las empresas que conforman el sector financiero estableciendo las bases para que las empresas financieras europeas minimicen los riesgos operacionales derivados de la utilización de las nuevas tecnologías.

El instrumento utilizado es el Reglamento de Resiliencia Operativa Digital, más conocido como Reglamento DORA.

Introducción

El Reglamento DORA amplía el foco del análisis de los riesgos de una entidad, hasta ahora muy centrado en la solvencia financiera, a nuevos riesgos operacionales y legales relacionados con el uso de las tecnologías, la ciberseguridad y la protección de los datos, entre otros.

Situación Actual

El pasado mes de mayo el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea llegaron a llegaron a un acuerdo definitivo sobre el Reglamento DORA.

El acuerdo ha sido aprobado por el Parlamento Europeo en la sesión plenaria del día 10 de noviembre, fue adoptado formalmente por el Consejo el día 28 de noviembre y ahora está pendiente de que se publique en el Diario Oficial.

Ese hecho se espera para el próximo mes de enero o febrero.

Objetivos del Reglamento DORA

Debido al riesgo cada vez mayor de ataques cibernéticos, la UE tiene como objetivo fortalecer la seguridad informática de las instituciones financieras como **bancos, compañías de seguros y empresas de inversión** por medio de DORA.

DORA tiene como objetivo garantizar que el sector financiero europeo pueda continuar operando con resiliencia en caso de interrupciones operativas graves

Objetivos del Reglamento DORA

DORA establece requisitos uniformes para la seguridad de las redes y los sistemas de información de las empresas y organizaciones que operan en el sector financiero y de terceros críticos que les brindan servicios relacionados con las TIC, como las plataformas en la nube.

DORA crea un marco regulatorio para la resiliencia operativa digital, lo que significa que todas las empresas que se encuentran dentro de su alcance deben asegurarse de poder resistir, responder y recuperarse de las interrupciones y amenazas relacionadas con las TIC

Entidades obligadas

(a) entidades de crédito,
(b) entidades de pago,
(c) entidades de dinero electrónico,
(d) empresas de servicios de inversión,
(e) proveedores de servicios de criptoactivos
(f) depositarios centrales de valores,
(g) entidades de contrapartida central,
(h) centros de negociación,
(i) registros de operaciones,
(j) gestores de fondos de inversión alternativos,
(k) sociedades de gestión,
(l) proveedores de servicios de suministro de datos,
(m) empresas de seguros y de reaseguros,
(n) intermediarios de seguros, reaseguros y seguros complementarios,
(o) fondos de pensiones de jubilación,
(p) agencias de calificación crediticia,
(r) administradores de índices de referencia cruciales,
(s) proveedores de servicios de financiación participativa,
(t) registros de titulizaciones,
(u) proveedores terceros de servicios de TIC.

Entidades excepcionadas

Están excluidas las empresas de seguros y reaseguros a que se refiere el artículo 4 de la Directiva 2009/138/CE que recoge las exclusiones del ámbito de aplicación de Solvencia II en razón de las dimensiones.

Las empresas de seguros y reaseguros que están excluidos de Solvencia II por dimensión también lo están de DORA

Están excluidos los intermediarios de seguros, de reaseguros o de seguros auxiliares que sean microempresas, o que sean pequeñas o medianas empresas.

La categoría de microempresas, pequeñas y medianas empresas (pymes) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones EUR o cuyo balance general anual no excede de 43 millones EUR

2. El Reglamento de Resiliencia Operativa Digital

El Reglamento se estructura en 5 Pilares

Formalmente la norma tiene 56 artículos distribuidos en 9 capítulos aunque desde la perspectiva de su contenido material, se habla de que está estructurada en cinco pilares:

1. Gestión de riesgos de TIC (artículos 4-14a)

2. Incidentes relacionados con las TIC. Gestión, clasificación e información (artículos 15-20a)

3. Pruebas de resiliencia operativa digital (artículos 21-24)

4. Gestión del riesgo de terceros en relación con las TIC (artículos 25-39)

5. Acuerdos de intercambio de información (artículo 40)

Gestión de riesgos TIC

¿Por qué?

Garantizar que **existen medidas y controles específicos para limitar la interrupción del mercado** y de los consumidores causada por incidentes, **y garantizar la rendición de cuentas del órgano de administración sobre la gestión de riesgos de TIC**.

Requisitos clave

Las empresas deberán **seguir los principios de gobernanza** en torno al riesgo de las TIC, **centrándose en la responsabilidad del órgano de administración**. Deberán identificar su **tolerancia al riesgo** de las TIC, en función del **apetito por el riesgo** de la organización y la **tolerancia al impacto** de las interrupciones de las TIC. También deberán contar con un **marco de gestión de riesgos** que incluya la identificación de **funciones críticas e importantes**, los riesgos asociados y un mapeo de los activos de TIC que los respaldan; así como protección específica, prevención, planes y capacidades de detección, respuesta y recuperación, procesos y métricas de mejora continua, y una estrategia de comunicación de crisis con funciones y responsabilidades claras.

Desafío más grande

Como parte de los procesos de mejora continua, DORA introduce **formación obligatoria sobre resiliencia operativa digital para el órgano de dirección pero también para todo el personal**, como parte de su paquete de formación general.

Reporte y gestión de incidentes TIC

¿Por qué?

Armonizar y centralizar el reporte de incidentes para **permitir que el regulador reaccione rápido para evitar la propagación del impacto** y para promover la mejora colectiva y el conocimiento de las empresas de las amenazas actuales al mercado.

Requisitos clave

DORA introduce una metodología estándar de clasificación de incidentes con un conjunto de criterios específicos (número de usuarios afectados, duración, distribución geográfica, pérdida de datos, gravedad del impacto en los sistemas TIC, criticidad de los servicios afectados, impacto económico) con umbrales que aún no se han publicado. Siguiendo esta metodología, los **incidentes** clasificados como **mayores** deberán ser **informados al regulador dentro del mismo día hábil**, siguiendo una plantilla determinada. También se requerirán **informes de seguimiento** después de **una semana** y después de **un mes**. Todos estos informes serán anonimizados, compilados y publicados periódicamente para toda la comunidad.

Desafío más grande

Las empresas deberán **cambiar su metodología de clasificación de incidentes** para ajustarse a los requisitos. También deberán establecer los procesos y canales correctos para poder notificar rápidamente al regulador en caso de que ocurra un incidente importante. Según lo que se clasifique como "principal", esto puede suceder con frecuencia.

Pruebas de resiliencia operativa digital

¿Por qué?

Garantizar que las entidades financieras **prueben la eficiencia del marco de gestión de riesgos y las medidas implementadas para responder y recuperarse de una amplia gama de escenarios de incidentes** de TIC, con una interrupción mínima de las funciones críticas e importantes, de una manera que sea proporcional a sus necesidades. tamaño y criticidad para el mercado.

Requisitos clave

Con DORA, todas las empresas deben **implementar un programa integral de pruebas**, que incluya una variedad de **evaluaciones, pruebas, metodologías, prácticas y herramienta**s, con un enfoque en las pruebas técnicas.

Las **empresas más críticas** también tendrán que organizar una **prueba de penetración en vivo dirigida por amenazas a gran escala cada 3 años** (ejercicio de tipo equipo rojo), realizada por **probadores independientes**, cubriendo **funciones y servicios críticos** e involucrando a terceros de TIC con sede en la UE. **El escenario deberá ser acordado previamente por el regulador** y las empresas recibirán un certificado de cumplimiento al finalizar la prueba.

Pruebas de resiliencia operativa digital

Desafío más grande

Es probable que las empresas críticas deban organizar esta prueba de penetración dirigida por amenazas para fines de 2025 y este tipo de prueba requiere mucha preparación (Marco TIIBER-ES).

El hecho de que necesite involucrar a terceros críticos de TIC también significará que ellos deben participar en la preparación. Las empresas que creen que estarán dentro del alcance deben comenzar a pensar en el escenario lo antes posible para permitir la validación con el regulador.

Gestión de riesgos de terceros

¿Por qué?

Asegurar que las organizaciones financieras tengan **un nivel adecuado de control y monitoreo de sus terceros TIC, especialmente aquellos que sustentan funciones críticas**; y establecer una supervisión específica sobre los proveedores que son críticos para el mercado en su conjunto.

Requisitos clave

Con este reglamento, la UE introduce requisitos tanto para las organizaciones financieras como para los proveedores críticos de TIC.

Las organizaciones financieras **deberán tener una estrategia y una política definidas de riesgo de terceros de TIC, evaluar el riesgo de concentración y de dependencia**. Deberán **compilar un registro estándar de información** que contenga una visión completa de todos sus proveedores externos de TIC, los servicios que brindan y las funciones que respaldan; e **informar sobre los cambios en este registro al regulador una vez al año**.

Gestión de riesgos de terceros

Requisitos clave

Deberán **evaluar a los proveedores de servicios de TIC** de acuerdo con ciertos criterios **antes de firmar un contrato** (por ejemplo, nivel de seguridad, riesgo de concentración, riesgos de subcontratación) y deberán **planificar una estrategia de salida** en caso de que un proveedor falle. DORA también **contiene pautas para el contenido del contrato. y motivos de terminación del contrato, que tiene que estar vinculado a un riesgo o evidencia de incumplimiento** a nivel del proveedor.

Bajo un nuevo Marco de Supervisión, los **proveedores críticos serán objeto de evaluaciones anuales contra los requisitos de resiliencia** tales como disponibilidad, continuidad, integridad de datos, seguridad física, procesos de gestión de riesgos, gobernanza, informes, portabilidad, pruebas. Estas evaluaciones se realizarán directamente por el regulador y dará lugar a sanciones por incumplimiento.

Desafío más grande

Recopilar información sobre todos los proveedores de TIC (no solo los más críticos), con **los servicios prestados y las funciones que respaldan para el registro de información** será una tarea muy grande para las grandes organizaciones financieras que generalmente dependen de miles de proveedores grandes y pequeños y contratos heredados, sistemas de gestión que dificultan la extracción de datos de archivos, etc.

Compartiendo información

¿Por qué?

Promover el intercambio de información e inteligencia sobre amenazas cibernéticas entre las organizaciones financieras para que puedan estar mejor preparadas.

Requisitos clave

DORA introduce directrices sobre el establecimiento de acuerdos de intercambio de información entre empresas para amenazas cibernéticas, incluidos los requisitos de confidencialidad y la necesidad de notificar al regulador.

Desafío más grande

Será una oportunidad para visibilizar iniciativas, redes o asociaciones locales y animar a más empresas a formar parte de ellas.

3. Síntesis de las obligaciones de DORA

Ampliar el Sistema de Gobierno

FIDES

Se residencia en el Consejo la responsabilidad de rendir cuentas al Supervisor sobre la adecuada capacidad de resiliencia operativa

Creación de 3 funciones:

- Para monitorizar los acuerdos celebrados con proveedores de servicios TIC
- Para administrar y supervisar los riesgos TIC
- Para gestionar las crisis

Elaboración de políticas y estrategias

- Política y procedimientos de seguridad
- Marco de gestión de riesgos de TIC sólido, completo y bien documentado como parte de su sistema general de gestión de riesgos
- Estrategia de resiliencia operativa digital que establezca cómo se aplica el marco de gestión de riesgos de TIC
- Continuidad del negocio TIC
- Modalidades de uso de servicios TIC de terceros
- Establecer y aplicar un marco de pruebas de la seguridad de la información llevadas a cabo de una manera segura y protegida por profesionales independientes

Ampliar el Sistema de Gobierno

Elaboración de inventarios accesibles al supervisor

- Registro de contratos sobre el uso de terceros proveedores TIC
- Registro de incidentes de seguridad
- Registro de las actividades antes, durante y después de eventos de interrupción

Auditorías independientes de:

- Marco de gestión de riesgos TIC
- Planes de respuesta y recuperación TIC asociadas
- Sobre los terceros proveedores TIC

Realización de pruebas periódicas del:

- Plan de continuidad TIC y planes de respuesta
- Plan de comunicación de crisis
- Plan de pruebas de escenarios de ciberataques
- Plan de contingencia y recuperación de desastres (especialmente el backup)
- Estrategias de salida de terceros TIC con recuperación y control de los datos en otro tercero o en infraestructura propia (funciones críticas o importantes)

Gestión ordinaria de sistemas

El reglamento DORA contiene más de un centenar de objetivos de control relacionados con los siguientes aspectos de la gestión:

- Gestión de los sistemas
- Seguridad física y lógica de los sistemas
- Detección de actividades anómalas
- Respuesta y recuperación a incidentes
- Planes de formación para personal interno y externo
- Gestión del riesgo de terceros y de la cadena de suministro
- Análisis exhaustivo previo a la celebración de un acuerdo contractual
- Operativa alrededor de los contratos de proveedores TIC
- Disposiciones contractuales clave obligatorias
- Revisiones, evaluaciones y pruebas de la seguridad de la información
- Pruebas de herramientas y sistemas TIC
- Gestión y notificación de incidentes

Gestión de riesgos TIC

Según las nuevas reglas, las empresas del sector financiero **deben desarrollar y mantener sistemas y herramientas** de TIC resilientes **que puedan identificar y mitigar los riesgos** de las TIC de **manera consistente y confiable**.

Cuando no estén ya obligados a hacerlo sobre la base de la legislación específica del sector, también tendrán que introducir **políticas integrales de continuidad del negocio** y **planes de recuperación ante desastres**.

DORA también **establece requisitos para los marcos de control y gobierno interno** que deben garantizar una gestión adecuada de todos los riesgos de TIC.

El **Consejo debe aprobar estos marcos, supervisar su implementación y es el responsable final**. Por lo tanto, se espera que **el Consejo desempeñe un papel activo y crucial en el cumplimiento de los requisitos** establecidos por DORA. Para fomentar el cumplimiento de esos requisitos, también se debe estimular la concienciación sobre los riesgos cibernéticos en todos los niveles de la organización. En este sentido, **las TIC ocupan un lugar explícito en la gobernanza** de las empresas financieras.

Gestión de riesgos TIC

Las entidades deberán contar con un marco de gestión de riesgos de TIC sólido, completo y bien documentado como parte de su sistema general de gestión de riesgos.

El marco de gestión de riesgos de TIC incluirá al menos estrategias, políticas, procedimientos, protocolos y herramientas de TIC que sean necesarios para proteger debida y adecuadamente todos los activos de información y activos de TIC

Las entidades que no sean microempresas deberán asignar la responsabilidad de administrar y supervisar los riesgos de TIC a una función de control y garantizar un nivel adecuado de independencia de dicha función de control para evitar conflictos de intereses. Podrá externalizarse.

El marco de gestión de riesgos de TIC se documentará y revisará al menos una vez al año. El supervisor podrá solicitar un informe sobre la revisión efectuada.

En las entidades no microempresas, el marco de gestión estará sujeto a auditorías internas periódicas por parte de auditores que posean suficientes conocimientos, habilidades y experiencia en riesgos de TIC. así como la adecuada independencia.

Gestión de riesgos TIC

El marco de gestión de riesgos de las TIC incluirá una **estrategia de resiliencia operativa digital** que establezca cómo se aplica el marco. A tal efecto, la estrategia de resiliencia operativa digital incluirá los métodos para abordar el riesgo de las TIC y lograr objetivos específicos de las TIC, mediante:

(a) La **explicación de cómo el marco de gestión de riesgos de TIC respalda la estrategia y los objetivos comerciales** de la entidad;
(b) El establecimiento del **límite de tolerancia al riesgo por riesgo TIC** de acuerdo con el apetito de riesgo de la entidad, y analizar la tolerancia al impacto por disrupciones TIC;
(c) El **establecimiento de objetivos claros de seguridad de la información**, incluidos **indicadores clave de rendimiento** y **métricas de riesgo clave**.
(d) La **explicación de la arquitectura de referencia de las TIC** y cualquier cambio necesario para alcanzar objetivos comerciales específicos;
(e) Esbozando los diferentes **mecanismos implementados para detectar, proteger y prevenir** los impactos de los incidentes relacionados con las TIC;
(f) Evidenciando la **situación actual de resiliencia operativa digital sobre la base del número de incidentes importantes** relacionados con las TIC notificados y la eficacia de las medidas preventivas;
(h) **Implementando pruebas de resiliencia operativa digital**, de conformidad con el Capítulo IV del DORA;
(i) Esbozando una **estrategia de comunicación en caso de incidentes** relacionados con las TIC que deban divulgarse de conformidad con el artículo 13.

Gestión de riesgos TIC

Las entidades financieras utilizarán y mantendrán actualizados los sistemas, protocolos y herramientas TIC.

Deberán mantener un inventario actualizado y revisado anualmente en el que:

- **identificarán, clasificarán y documentarán** adecuadamente **todas las funciones y responsabilidades comerciales** respaldadas por las TIC, **los activos de información y los activos de las TIC que respaldan** estas funciones.
- **identificarán todos los activos de información y activos TIC**, **incluidos los que se encuentran en sitios remotos, los recursos de red y los equipos de hardware, y mapearán los que se consideren críticos**. Mapearán la configuración de los activos de información y los activos de TIC y los vínculos e interdependencias entre los diferentes activos de información y los activos de TIC.
- **identificarán y documentarán todos los procesos que dependan de terceros proveedores de servicios de TIC** e identificarán las interconexiones con terceros proveedores de servicios de TIC que respalden funciones críticas o importantes.

Deberá hacerse una evaluación de riesgos cada vez que haya un cambio importante en la infraestructura y al menos anualmente en los sistemas legacy.

Gestión de riesgos TIC

Con el fin de proteger adecuadamente los sistemas TIC y con miras a organizar medidas de respuesta, las entidades **monitorearán y controlarán continuamente la seguridad y el funcionamiento de los sistemas y herramientas TIC** y minimizarán el impacto de tales riesgos TIC mediante el despliegue de las herramientas TIC apropiadas. herramientas, políticas y procedimientos de seguridad.

Las entidades financieras deberán diseñar, adquirir e implementar estrategias, políticas, procedimientos, protocolos y herramientas de seguridad de las TIC que apunten a garantizar la resiliencia, continuidad y disponibilidad de los sistemas de TIC, en particular para aquellos que respaldan funciones críticas o importantes.

Para ello utilizarán soluciones y procesos de TIC proporcionales que **permitan mantener altos estándares de confidencialidad,** integridad y disponibilidad de los datos, **ya sea en reposo, en uso o en tránsito**.

Gestión de riesgos TIC

En todos los aspectos relacionados con al seguridad física y lógica, los reuerimientos del Reglamento son:

a) definir, documentar e instaurar procedimientos para el control del acceso lógico o la seguridad lógica (gestión de la identidad y los accesos).
b) siguiendo un enfoque basado en el riesgo, establecer una gestión sólida de la red y la infraestructura utilizando técnicas, métodos y protocolos apropiados que pueden incluir la implementación de mecanismos automatizados para aislar los activos de información afectados en caso de ataques cibernéticos.
c) implementar políticas que limiten el acceso físico o lógico a los activos de TIC y activos de información a lo que se requiere únicamente para funciones y actividades legítimas y aprobadas, y establecer a tal efecto un conjunto de políticas, procedimientos y controles que aborden los privilegios de acceso y una buena administración de los mismos.
d) implementar políticas y protocolos para mecanismos de autenticación sólidos, basados en estándares relevantes y sistemas de control dedicados, y medidas de protección de claves criptográficas mediante las cuales los datos se cifran en función de los resultados de la clasificación de datos aprobada y los procesos de evaluación de riesgos de TIC.
e) implementar políticas, procedimientos y controles documentados para la gestión de cambios de TIC, incluidos los cambios de software, hardware, componentes de firmware, cambios de sistema o seguridad, que se basan en un enfoque de evaluación de riesgos y como parte integral del proceso general de gestión de cambios de la entidad financiera, para garantizar que todos los cambios en los sistemas de TIC se registren, prueben, evalúen, aprueben, implementen y verifiquen de manera controlada.
f) tener políticas documentadas apropiadas y completas para parches y actualizaciones

Reporte y gestión de incidentes TIC

DORA creará un canal de informes más optimizado para incidentes relacionados con las TIC, lo que es una consolidación bienvenida de los requisitos de informes múltiples actuales.

Se **reducirán los eventos desencadenantes** de informes y se armonizarán las plantillas de informes. Un **único centro** de la UE **recopilará todos los informes** de los principales eventos relacionados con las TIC que afecten a las entidades financieras. **Los datos recopilados revelarán cualquier tendencia de vulnerabilidad común** en todo el sector financiero para respaldar una mayor optimización de la resiliencia y la seguridad de las TIC.

De acuerdo con las nuevas reglas de informes de la UE, todas las empresas financieras **deberán presentar un informe de causa raíz dentro del mes posterior a un incidente** de TIC importante.

Para respaldar la presentación oportuna de dichos informes, las entidades financieras deberán **implementar indicadores confiables de alerta temprana** de las interrupciones de las TIC.

Reporte y gestión de incidentes TIC

Las entidades **establecerán una Política integral de continuidad del negocio de las TIC**, que podrá adoptarse como una política específica dedicada que forme parte integrante de la política general de continuidad del negocio. Las entidades implementarán esta Política a través de compromisos, planes, procedimientos y mecanismos específicos, apropiados y documentados destinados a:

- asegurar la continuidad de las funciones críticas o importantes de la entidad;

- responder y resolver de forma rápida, adecuada y eficaz todos los incidentes relacionados con las TIC, de forma que se limiten los daños y se priorice la reanudación de las actividades y las acciones de recuperación;

- activar sin demora planes específicos que permitan medidas, procesos y tecnologías de contención adecuados para cada tipo de incidente relacionado con las TIC y prevenir daños mayores, así como procedimientos personalizados de respuesta y recuperación establecidos;

- La estimación preliminar de impactos, daños y pérdidas;

- establecer acciones de comunicación y gestión de crisis que garanticen que la información actualizada se transmita a todo el personal interno pertinente y a las partes interesadas externas y se notifique a las autoridades competentes.

Los planes de respuesta y recuperación de TIC **asociados estarán sujetos a revisiones de auditoría interna independientes**.

Reporte y gestión de incidentes TIC

Como parte de su gestión integral de riesgos TIC, las entidades deberán:

(a) **probar los Planes de Continuidad del Negocio de TIC y los Planes de Respuesta y Recuperación de TIC** en relación con los sistemas de TIC que respaldan todas las funciones **al menos una vez al año**, así como sobre cualquier cambio sustancial en los sistemas de TIC que respaldan funciones críticas o importantes;
(b) **probar los planes de comunicación** de crisis establecidos.

Las entidades incluirán en los planes de prueba, **escenarios de ciberataques y cambios entre la infraestructura TIC primaria y la capacidad redundante, las copias de seguridad y las instalaciones redundantes necesarias para cumplir las obligaciones legales**.

Las entidades tendrán una **función de gestión de crisis** que, en caso de activación de sus planes de Continuidad del Negocio TIC o planes de respuesta y recuperación de TIC, deberá, entre otras cosas, establecer procedimientos claros para gestionar las comunicaciones de crisis internas y externas.

Las entidades deberán mantener registros fácilmente accesibles de las actividades antes y durante los eventos de interrupción cuando se activen sus planes de continuidad del negocio TIC y sus planes de respuesta y recuperación TIC y las entidades que no sean microempresas deberán informar a las autoridades competentes, previa solicitud, una estimación de los costes y pérdidas anuales agregados causados por incidentes importantes relacionados con las TIC.

La activación de los sistemas de respaldo no deberá poner en peligro la seguridad de la red y los sistemas de información ni la confidencialidad, integridad o disponibilidad de los datos. **Las pruebas de los procedimientos de copia de seguridad y restauración se realizarán periódicamente**.

Reporte y gestión de incidentes TIC

Las entidades desarrollarán **programas de concientización sobre la seguridad de las TIC y capacitaciones en resiliencia operativa digita**l como **módulos obligatorios en sus esquemas de capacitación del personal**.

¿Posibles consecuencias de no superar esa capacitación?

Serán aplicables a **todos los empleados y al personal de alta dirección, y tendrán un nivel de complejidad acorde con el ámbito de sus funciones**. En su caso, las entidades **también incluirán proveedores de servicios de TIC de terceros** en sus planes de formación pertinentes.

Las entidades **deberán monitorear los desarrollos tecnológicos relevantes de manera continua**, también con miras a comprender los posibles impactos del despliegue de tales nuevas tecnologías sobre los requisitos de seguridad de las TIC y la resiliencia operativa digital. **Se mantendrán al tanto de los últimos procesos de gestión de riesgos de las TIC**, contrarrestando eficazmente las formas actuales o nuevas de ciberataques.

¿Establecer un “observatorio” de la innovación tecnológica?

.

Resiliencia operativa digital

DORA establece estándares uniformes a lo largo de la UE para probar la resiliencia operativa digital.

Los requisitos de prueba incluyen evaluaciones de vulnerabilidad y seguridad de la red, análisis de brechas y pruebas de soluciones de software, así como pruebas basadas en escenarios, pruebas de rendimiento y pruebas de penetración.

Estos requisitos tienen como objetivo establecer un enfoque uniforme para los estándares de resiliencia operativa, poniéndolos dentro del alcance de la UE por primera vez.

Resiliencia operativa digital

Las empresas deberán **realizar diversas revisiones, evaluaciones y pruebas de la seguridad de la información** para garantizar la identificación eficaz de las vulnerabilidades en sus sistemas y servicios de TIC. Por ejemplo, las empresas podrán realizar análisis de deficiencias respecto de los estándares de seguridad de la información, revisiones del cumplimiento, auditorías internas y externas de los sistemas de información o revisiones de la seguridad física.

Las empresas **deberán establecer y aplicar un marco de pruebas de la seguridad de la información** que valide la solidez y la eficacia de sus medidas al respecto y garantizar que este marco considera las amenazas y vulnerabilidades identificadas mediante el seguimiento de amenazas y el proceso de evaluación de riesgos de TIC y seguridad.

Las pruebas se deberán llevar a cabo de una manera segura y protegida por profesionales independientes con el conocimiento, las capacidades y la experiencia suficientes en la realización de pruebas de medidas de seguridad de la información.

Las empresas deberán llevar a cabo **pruebas de manera periódica**. El alcance, la frecuencia y el método de las pruebas (como las pruebas de penetración, incluidas las pruebas de intrusión dirigida sobre amenaza (threat-led penetration testing) deberán ser acordes al nivel de riesgo detectado. Las pruebas de los sistemas de TIC esenciales y los análisis de vulnerabilidades se deberán llevar a cabo anualmente.

Las empresas deberán **garantizar que se realizan pruebas de las medidas de seguridad en el caso de cambios en la infraestructura, los procesos o procedimientos**; también si se realizan cambios derivados de importantes incidentes operativos o de seguridad o debido al lanzamiento de aplicaciones esenciales nuevas o modificadas de forma significativa.

Los acuerdos contractuales para la provisión de funciones críticas o importantes incluirán, además de lo anterior, al menos lo siguiente:

a) Las entidades financieras distintas de las microempresas, tienen que establecer, mantener y revisar un programa sólido y completo de pruebas de resiliencia operativa digital como parte integral del marco de gestión de riesgos de TIC.
b) El programa de pruebas de resiliencia operativa digital incluirá una serie de evaluaciones, pruebas, metodologías, prácticas y herramientas.
c) Las entidades se asegurarán de que las pruebas sean realizadas por partes independientes, ya sean internas o externas. Cuando las pruebas sean realizadas por un evaluador interno, las entidades financieras deberán dedicar suficientes recursos y garantizar que se eviten los conflictos de interés durante las fases de diseño y ejecución de la prueba.
d) Las entidades establecerán procedimientos y políticas para priorizar, clasificar y remediar todos los problemas reconocidos a lo largo de la realización de las pruebas y establecerán metodologías de validación interna para asegurarse de que todas las debilidades, deficiencias o lagunas identificadas se solucionen por completo.
e) Las entidades se asegurarán de que se realicen las pruebas adecuadas en todos los sistemas y aplicaciones de TIC críticos al menos una vez al año

Resiliencia operativa digital

El programa de prueba de resiliencia operativa digital permitirá la ejecución de pruebas adecuadas, como evaluaciones y escaneos de vulnerabilidad, análisis de fuente abierta, evaluaciones de seguridad de la red, análisis de brechas, revisiones de seguridad física, cuestionarios y soluciones de software de escaneo, revisiones de código fuente cuando sea factible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo o pruebas de penetración.

Las entidades **realizarán evaluaciones de vulnerabilidad antes de cualquier despliegue o redespliegue de servicios** nuevos o existentes que apoyen las funciones, aplicaciones y componentes de infraestructura críticos de la entidad;

Las entidades distintas de las microempresas y las pequeñas empresas no interconectadas, que no estén exceptuadas, llevarán a cabo, **al menos cada tres años, pruebas avanzadas mediante pruebas de penetración basadas en amenazas**. Con base en el perfil de riesgo de la entidad financiera y tomando en cuenta las circunstancias operativas, la autoridad competente podrá, cuando sea necesario, solicitar a la entidad financiera que reduzca o amplíe esta frecuencia.

Cada prueba de penetración dirigida por amenazas cubrirá varias o todas las funciones y servicios críticos o importantes de una entidad, y se realizará en sistemas de producción en vivo que respalden dichas funciones. El alcance preciso de las pruebas de penetración dirigidas por amenazas, basado en la evaluación de funciones y servicios críticos o importantes, será determinado por las entidades financieras y validado por las autoridades competentes.

Cuando los terceros proveedores de servicios de TIC estén incluidos en el ámbito de las pruebas de penetración dirigidas por amenazas, la entidad financiera tomará las medidas y salvaguardas necesarias para garantizar la participación de dichos terceros proveedores de servicios de TIC.

Gestión de riesgos de terceros

DORA estipula que los **proveedores de TIC**, incluidos los proveedores de servicios en la nube, **estarán regulados por una de las Autoridades Europeas de Supervisión** (ESA), que tendrá el poder de solicitar información, hacer recomendaciones y solicitudes, realizar inspecciones e incluso imponer sanciones por incumplimiento de las nuevas normas de la UE sobre gestión de riesgos y resiliencia operativa.

Las empresas financieras también **deberán evaluar y documentar todos los riesgos potenciales asociados con sus proveedores de servicios TIC** externos **y asegurarse de que sus contratos con dichas empresas especifiquen sus obligaciones legales en virtud de la nueva legislación**.

DORA también tiene un impacto en los proveedores de servicios de terceros países: **los proveedores críticos de servicios de TIC** para las entidades financieras de la UE establecidas en terceros países **tendrán que establecer una filial dentro de la UE**, para que pueda ser supervisado adecuadamente.

Gestión de riesgos de terceros

Para garantizar un control sólido del riesgo de terceros de TIC, es necesario **establecer un conjunto de reglas basadas en principios para guiar a las entidades cuando controlen el riesgo que surge en el contexto de las funciones subcontratadas a proveedores de servicios de terceros de TIC**.

En particular para los servicios de TIC que respaldan las funciones críticas o importantes, así como, de manera más general, en el contexto de todas las dependencias de terceros de TIC.

Las entidades financieras **deben aplicar un enfoque proporcionado al seguimiento de los riesgos que surjan a nivel de terceros proveedores de servicios de TIC**, teniendo debidamente en cuenta la naturaleza, escala, complejidad e importancia de sus dependencias relacionadas con las TIC, la criticidad o importancia de los servicios, procesos o funciones sujetos a los acuerdos contractuales y, en última instancia, sobre la base de una evaluación cuidadosa de cualquier impacto potencial en la continuidad y calidad de los servicios financieros a nivel individual y de grupo, según corresponda.

Gestión de riesgos de terceros

La realización de dicho monitoreo debe seguir un enfoque estratégico del riesgo de terceros de TIC formalizado a través de la **adopción por parte del órgano de administración de la entidad financiera de una estrategia de riesgo de terceros de TIC** basada en una **evaluación continua de todas esas dependencias** de terceros de TIC.

Las entidades están obligadas a mantener un **Registro de Información con todos los acuerdos contractuales sobre el uso de servicios de TIC** proporcionados por terceros proveedores de servicios de TIC.

Los supervisores financieros pueden solicitar el registro completo o solicitar secciones específicas del mismo, y así obtener información esencial para adquirir una comprensión más amplia de las dependencias TIC de las entidades financieras.

Las entidades **reportarán al menos una vez al año a las autoridades competentes**, información sobre el número de nuevos contratos sobre el uso de servicios TIC, las categorías de terceros proveedores de servicios TIC, el tipo de acuerdos contractuales y los servicios y funciones que se están proporcionando.

Gestión de riesgos de terceros

Un **análisis exhaustivo previo a la contratación** debe respaldar y preceder a la conclusión formal de los acuerdos contractuales.

Antes de celebrar un acuerdo contractual sobre el uso de servicios TIC, las entidades financieras deberán:

(a) evaluar si el acuerdo contractual cubre el uso de servicios de TIC relacionados con una función crítica o importante;

(b) evaluar si se cumplen las condiciones de supervisión para la contratación;

(c) identificar y evaluar todos los riesgos pertinentes en relación con el acuerdo contractual, incluida la posibilidad de que dichos acuerdos contractuales puedan contribuir a reforzar el riesgo de concentración relacionado con las TIC;

(d) llevar a cabo toda la diligencia debida con respecto a los posibles proveedores de servicios de terceros de TIC y garantizar durante los procesos de selección y evaluación que el proveedor de servicios de terceros de TIC es adecuado;

(e) identificar y evaluar los conflictos de interés que el acuerdo contractual pueda causar.

Gestión de riesgos de terceros

Las entidades financieras **solo pueden celebrar acuerdos contractuales con terceros proveedores de servicios de TIC que cumplan con los estándares apropiados de seguridad** de la información (Requerir cumplimiento de estándares ISO, ENS, etc.).

Para ejercer los **derechos de acceso, inspección y auditoría sobre el tercero proveedor** de servicios de TIC, las entidades **deberán**, con un enfoque basado en el riesgo, **predeterminar la frecuencia de las auditorías e inspecciones y las áreas a auditar** mediante el cumplimiento de normas comunes.

Cuando los acuerdos contractuales concluidos con terceros proveedores de servicios de TIC sobre el uso de servicios de TIC impliquen una gran complejidad técnica, la entidad verificará que los auditores, ya sean auditores internos o externos o un grupo de auditores, posean las habilidades y los conocimientos adecuados para desempeñar auditorías y evaluaciones.

Gestión de riesgos de terceros

Las entidades financieras **solo pueden celebrar acuerdos contractuales con terceros proveedores de servicios de TIC que cumplan con los estándares apropiados de seguridad** de la información (Requerir cumplimiento de estándares ISO, ENS, etc.).

Para ejercer los **derechos de acceso, inspección y auditoría sobre el tercero proveedor** de servicios de TIC, las entidades **deberán**, con un enfoque basado en el riesgo, **predeterminar la frecuencia de las auditorías e inspecciones y las áreas a auditar** mediante el cumplimiento de normas comunes.

En el uso de servicios de TIC que impliquen una gran complejidad técnica, la entidad verificará que los auditores posean las habilidades y los conocimientos adecuados para desempeñar auditorías y evaluaciones.

Para los servicios de TIC relacionados con funciones críticas o importantes, las entidades **deberán establecer estrategias de salida y los planes de salida serán exhaustivos, documentados, suficientemente probados y revisados periódicamente.**

Gestión de riesgos de terceros

Las entidades identificarán soluciones alternativas y **desarrollarán planes de transición que les permitan eliminar las funciones contratadas y los datos relevantes** de las TIC tercero proveedor de servicios **y transferirlos de forma segura e integral a proveedores alternativos o reincorporarlos internamente**.

Las entidades adoptarán las medidas de contingencia adecuadas para mantener la continuidad del negocio en todas las circunstancias mencionadas.

Cuando se celebren acuerdos contractuales sobre el uso de servicios de TIC relativos a funciones críticas o importantes con un tercero proveedor de servicios de TIC, las entidades financieras considerarán debidamente las disposiciones de la legislación sobre insolvencia que se aplicarían en caso de quiebra del tercero proveedor de servicios de TIC como así como cualquier limitación que pudiera surgir respecto de la recuperación urgente de los datos de la entidad financiera.

Gestión de riesgos de terceros

Al realizar la identificación y evaluación del riesgo de concentración de TIC, las entidades tendrán en cuenta si la celebración de un acuerdo contractual en relación con los servicios de TIC que respaldan funciones críticas o importantes daría lugar a cualquiera de las siguientes situaciones:

(a) **contratar a un tercero** proveedor de servicios de TIC **que no sea fácilmente sustituible**; o
(b) **tener en vigor múltiples acuerdos contractuales** en relación con la prestación de servicios de TIC **que respalden funciones críticas o importantes con el mismo proveedor** de servicios de terceros de TIC **o con proveedores** de servicios de terceros de TIC **estrechamente conectados**.

Las entidades **sopesarán los beneficios y los costes de las soluciones alternativas**, como el uso de diferentes proveedores de servicios externos de TIC, teniendo en cuenta si las soluciones previstas se ajustan a las necesidades y objetivos empresariales establecidos en su estrategia de resiliencia digital y de qué manera.

Cuando el acuerdo contractual sobre el uso de servicios TIC que respalden funciones críticas o importantes **incluya** la posibilidad de que un **tercero proveedor de servicios TIC subcontrate una función crítica o importante a otros terceros proveedores de servicios TIC**, las entidades sopesarán los beneficios y los riesgos que pueden surgir en relación con dicha posible subcontratación, en particular en el caso de un subcontratista de TIC establecido en un tercer país. Se **deberá evaluar si las cadenas de subcontratación potencialmente largas o complejas pueden afectar su capacidad para monitorear completamente las funciones contratadas** y la capacidad de la autoridad competente para supervisar efectivamente a la entidad financiera en ese sentido.

Gestión de riesgos de terceros

Al realizar la identificación y evaluación del riesgo de concentración de TIC, las entidades tendrán en cuenta si la celebración de un acuerdo contractual en relación con los servicios de TIC que respaldan funciones críticas o importantes daría lugar a cualquiera de las siguientes situaciones:

(a) **contratar a un tercero** proveedor de servicios de TIC **que no sea fácilmente sustituible**; o
(b) **tener en vigor múltiples acuerdos contractuales** en relación con la prestación de servicios de TIC **que respalden funciones críticas o importantes con el mismo proveedor** de servicios de terceros de TIC **o con proveedores** de servicios de terceros de TIC **estrechamente conectados**.

Las entidades **sopesarán los beneficios y los costes de las soluciones alternativas**, como el uso de diferentes proveedores de servicios externos de TIC, teniendo en cuenta si las soluciones previstas se ajustan a las necesidades y objetivos empresariales establecidos en su estrategia de resiliencia digital y de qué manera.

Cuando el acuerdo contractual sobre el uso de servicios TIC que respalden funciones críticas o importantes **incluya** la posibilidad de que un **tercero proveedor de servicios TIC subcontrate una función crítica o importante a otros terceros proveedores de servicios TIC**, las entidades sopesarán los beneficios y los riesgos que pueden surgir en relación con dicha posible subcontratación, en particular en el caso de un subcontratista de TIC establecido en un tercer país. Se **deberá evaluar si las cadenas de subcontratación potencialmente largas o complejas pueden afectar su capacidad para monitorear completamente las funciones contratadas** y la capacidad de la autoridad competente para supervisar efectivamente a la entidad financiera en ese sentido.

Gestión de riesgos de terceros

Los derechos y obligaciones de las partes deberán estar claramente asignados y establecidos por escrito en un contrato que incluirá los acuerdos de nivel de servicio y se documentará en un documento disponible para las partes en papel, o en un documento con otro formato descargable, duradero y accesible.

Los acuerdos contractuales sobre el uso de los servicios TIC incluirán, al menos, lo siguiente:

- una **descripción clara y completa de todas las funciones y servicios que prestará el tercero**, indicando si está permitida la subcontratación de una función crítica o importante, o partes importantes de la misma, y, en caso afirmativo, las condiciones que se aplican a tal subcontratación.
- **las ubicaciones**, es decir, las regiones o países, **donde se prestarán las funciones** contratadas o subcontratadas y los servicios de TIC **y donde se procesarán los datos**, **incluida la ubicación de almacenamiento**, y el requisito de que el tercero proveedor de servicios de TIC notifique con antelación la entidad financiera si tiene previsto cambiar dichos lugares.
- **disposiciones sobre accesibilidad, disponibilidad, integridad, seguridad, confidencialidad y protección de datos**, incluidos los datos personales.
- **disposiciones para garantizar el acceso, la recuperación y la devolución en un formato de fácil acceso de los datos** personales y no personales procesados por la entidad financiera en caso de insolvencia, resolución o interrupción de las operaciones comerciales del tercero proveedor de servicios de TIC, o en el caso de terminación de los acuerdos contractuales.
- **descripciones de niveles de servicio**, incluidas actualizaciones y revisiones de los mismos.
- **la obligación del tercero** proveedor **de prestar asistencia en caso de un incidente** relacionado con las TIC relacionado con el servicio prestado **sin coste adicional o con un coste determinado ex-ante**.
- la obligación del tercero de cooperar plenamente con las autoridades competentes y las autoridades de resolución de la entidad, incluidas las personas designadas por ellas.

Gestión de riesgos de terceros

Los **acuerdos** contractuales **para la provisión de funciones críticas o importantes** incluirán, además de lo anterior, al menos lo siguiente:

- **descripciones completas de los niveles de servicio**, incluidas las actualizaciones y revisiones de los mismos con objetivos de desempeño cuantitativos y cualitativos precisos dentro de los niveles de servicio acordados para permitir un control efectivo por parte de la entidad financiera y permitir sin demoras indebidas que se tomen las medidas correctivas apropiadas cuando no se cumplan los niveles de servicio acordados;
- **períodos de notificación y obligaciones de información del tercero** a la entidad, incluida la notificación de cualquier desarrollo que pueda tener un impacto material en la capacidad del tercero proveedor de para llevar a cabo de manera efectiva funciones críticas o importantes de acuerdo con lo acordado;
- **requisitos para que el tercero implemente y pruebe planes de contingencia comercial** y tenga implementadas medidas, herramientas y políticas de seguridad de TIC que brinden un nivel adecuado de prestación segura de servicios por parte de la entidad financiera de acuerdo con su marco regulatorio;
- **la obligación del tercero de participar y cooperar plenamente en una prueba de penetración de amenazas** de la entidad;
- **el derecho a monitorear de manera continua el desempeño del proveedor** de servicios de TIC;
- **estrategias de salida, en particular el establecimiento de un período de transición obligatorio adecuado**;

Al negociar acuerdos contractuales, las entidades y los terceros proveedores de servicios de TIC **deberán considerar el uso de cláusulas contractuales estándar desarrolladas por las autoridades públicas** para servicios específicos.

Compartiendo información

DORA alienta a las empresas financieras a compartir información e inteligencia sobre ciberseguridad con empresas de otros Estados miembros, en un esfuerzo por reducir el impacto de las amenazas cibernéticas en los servicios financieros y fortalecer las capacidades de respuesta y recuperación en el sector financiero europeo en su conjunto.

4. Responsabilidades del Consejo de Administración

Responsabilidades directas del Consejo

1. Definir, aprobar y supervisar la implementación de todos los acuerdos relacionados con el marco de gestión de riesgos de TIC y es responsable último de la gestión de los riesgos TIC. **Establecer funciones y responsabilidades claras** para todas las funciones relacionadas con las TIC.

2. **Establecer y aprobar la estrategia de resiliencia operativa digital**, incluida la determinación del nivel adecuado de tolerancia al riesgo de TIC.

3. **Aprobar, supervisar y revisar** periódicamente la implementación de la **Política de Continuidad del Negocio TIC**.

4. **Aprobar y revisar** periódicamente **los planes de auditoría interna** TIC de la entidad, las auditorías TIC y sus modificaciones materiales.

5. **Asignar y revisar** periódicamente el **presupuesto adecuado** para satisfacer las necesidades de resiliencia operativa digital.

Responsabilidades directas del Consejo

6. Aprobar y revisar periódicamente la **política de la entidad sobre las modalidades de uso de los servicios TIC prestados por terceros.**

7. Ser **informado de los acuerdos celebrados con terceros** proveedores de servicios de TIC.

8. Las entidades que no sean microempresas deberán establecer una **función para monitorizar los acuerdos celebrados con terceros proveedores de servicios** de TIC sobre el uso de servicios de TIC, **o deberán designar a un miembro de la alta gerencia como responsable** de supervisar la exposición al riesgo relacionado y la documentación relevante.

9. Los **miembros del órgano de administración** de la entidad financiera **deberán mantener activamente actualizados los conocimientos y habilidades suficientes** para comprender y evaluar los riesgos de las TIC y su impacto en las operaciones de la entidad financiera, **incluso siguiendo una formación específica de forma regular**, acorde con riesgos TIC que se gestionan.

5. Calendario de implantación

Calendario de implantación

Aprobación por el Parlamento Europeo en sesión plenaria

Publicación en el D.O. y entrada en vigor

WorkShop de EIOPA con la Industria

Publicación de normas técnicas obligatorias:
- Sobre procedimientos de clasificación de incidentes TIC y ciberamenazas.
- Sobre el nivel de detalle requerido en las estrategias del riesgos de terceros de TIC de las empresas
- Otros elementos del marco de gestión de riesgos de las TIC
- Registro de Información sobre Acuerdos Contractuales de Terceros TIC

Publicación de normas técnicas obligatorias:
- Sobre la notificación de los principales incidentes cibernéticos y de TIC a las autoridades
- Sobre alcance y elementos adicionales para requisitos de prueba avanzados
- Sobre disposiciones contractuales clave para la subcontratación de funciones que respaldan las FCI

Exigibilidad de su pleno cumplimiento

12 meses

18 meses

24 meses

10-nov-22

febrero-23

marzo-23

febrero-24

octubre-24

febrero-25

2022 | 2023 | 2024 | 2025

GRACIAS POR SU ATENCIÓN