ASEAFI

ASOCIACIÓN DE EMPRESAS DE ASESORAMIENTO FINANCIERO

CONGRESO ANUAL ASEAFI 2023

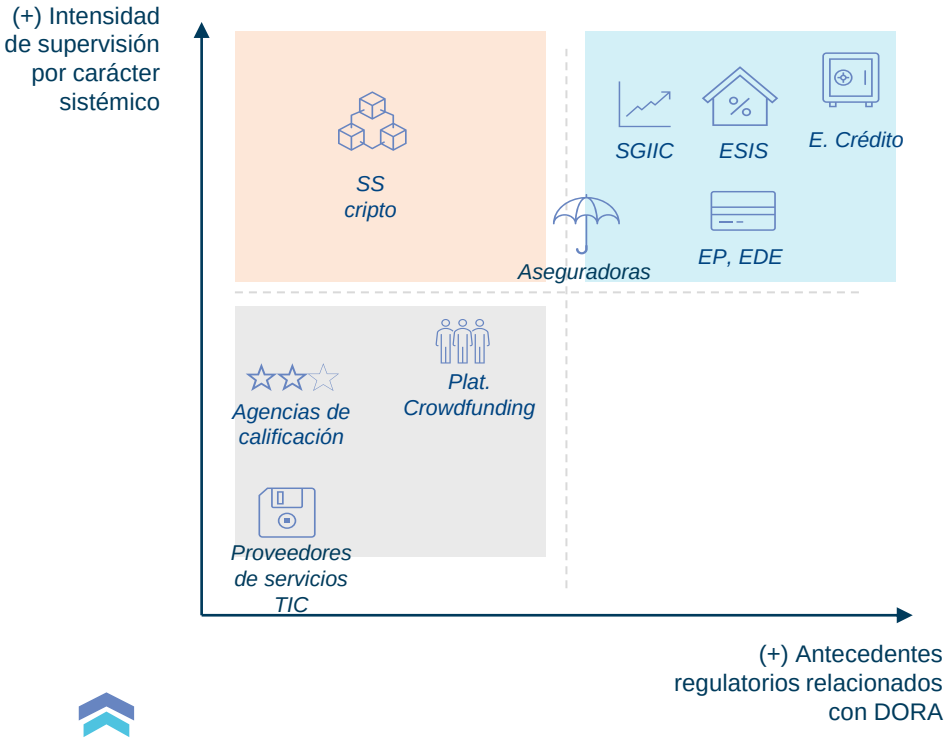
DORA: Principales Impactos

Junio 2023

finReg360

DORA aplica a diferentes entidades, por su implicación en el ámbito de la resiliencia digital

Matriz de madurez DORA, estimada para cada tipo de entidad



Como consecuencia del **carácter sistémico de las entidades de crédito,** éstas han estado sometidas a una mayor carga de supervisión y regulatoria que han permitido que **algunos de requerimientos de DORA ya se encuentren implementados**, a pesar de que pueda existir **falta de homogeneidad en el enfoque adoptado** por las entidades.

Racional regulatorio por entidad

Entidad	Antecedentes regulatorios	Intensidad de supervisión
E. Crédito	• Guías EBA: • ICT • Externalización • Gobierno interno	• BdE, ECB, EBA, SRB
EP, EDE		• BdE, ECB EBA
ESIS		• CNMV, ESMA
SGIIC		• CNMV, EFAMA
Compañías Aseguradoras	-	• DGSFP, EIOPA
SS Cripto	-	• BdE, CNMV
Plataformas Crowdfunding	-	• CNMV
Agencias de calificación	-	• CNMV, ESMA
Proveedores SS TIC	-	-

Quedan fuera del ámbito de aplicación de DORA

Entidad	Detalle
Gestores de fondos de inversión alternativos tal como se contempla en el art.3.2 la Directiva 2011/61/UE relativa a los gestores de fondos de inversión alternativos	Los GFIA que, directa o indirectamente, a través de una empresa con la que el GFIA esté relacionado por motivos de gestión o control común, o por la participación directa o indirecta sustancial, gestionen carteras de FIA: ○ **cuyos activos gestionados, incluidos activos adquiridos mediante recursos de apalancamiento, no rebasen en total un umbral de 100M€.** ○ **Cuyos activos gestionados no rebasen en total un umbral de 500M€, cuando las carteras de los FIA consistan en FIA que no están apalancados y no tengan derechos de reembolso que puedan ejercerse durante un periodo de cinco años después de la fecha de inversión inicial en cada FIA.**
Empresas de seguros y reaseguros tal como se contemplan en el **art. 4 de la Directiva 2009/138/CE sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio** (Solvencia II)	Empresas de seguros que cumplan todas las siguientes condiciones: • **Ingresos anuales brutos por primas escritas < 5.000.000€,** • Total de **provisiones técnicas de la empresa**, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial **< 25.000.000€** • Cuando pertenezca a un **grupo, el total de las provisiones técnicas del grupo**, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial **< 25.000.000€** • Cuando sus actividades **no incluyen seguros o reaseguros que cubren riesgos de pasivos, créditos y cauciones** salvo que constituyan riesgos accesorios. • Las actividades **no incluyen operaciones de reaseguro** que: ○ **Excedan de 500.000€ o más del 10%** de sus ingresos anuales brutos por primas escritas, o ○ **Excedan de 2.500.000€ o más del 10%** de sus provisiones técnicas, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial
Otros	• Fondos de pensiones de empleo que gestionen planes de pensiones que, en su conjunto, no tengan más de 15 partícipes en total • Oficinas de cheques postales

Asimismo, DORA no se aplicará a las siguientes entidades

Entidad	Detalle
Personas físicas o jurídicas exentas en virtud del art.2 y art.3 de la Directiva 2014/65/UE relativa a los mercados de instrumentos financieros	• Entidades **exentas de la aplicación de la Directiva 2014/65/UE MiFID**

Intermediarios de seguros, de reaseguros y de seguros complementarios que sean microempresas o pequeñas o medianas empresas	• **Microempresa** es aquella que:
	  ○ Ocupen a < 10 personas, y
	  ○ Cuyo volumen de negocio anual o cuyo balance < 2M€.
	• **Pequeña empresa** es aquella que:
	  ○ ocupen a > 10 personas y < 50 personas, y
	  ○ Cuyo volumen de negocio anual o cuyo balance sea > 2M€ y < 10M€.
	• **Medianas empresas** es una entidad financiera distinta de una pequeña empresa que:
	  ○ Ocupen a < 250 personas, y
	  ○ Cuyo volumen de negocio anual < 50M€, o cuyo balance < 43M€.

Adicionalmente,	España podrá excluir al Instituto de Crédito Oficial. En caso de excluirlo, deberá, informar de ello a la Comisión, así como de cualquier modificación posterior al respecto.

Objetivos concretos en el ámbito de resiliencia operativa digital

DORA

Objetivos

Establecer **requisitos uniformes relativos a la seguridad de las redes y los sistemas de información** que sustentan los procesos empresariales de las entidades financieras, los cuales son necesarios para lograr un elevado nivel común de resiliencia operativa digital

Contenido

a) Requisitos **aplicables a las entidades financieras** en relación con:

- la **gestión de riesgos** en el ámbito de las tecnologías de la información y la comunicación (TIC)
- la **notificación de incidentes** graves y **ciberamenazas** relacionados con las TIC, así como los de **pagos** a las autoridades competentes
- las **pruebas de resiliencia** operativa digital
- el **intercambio de información** e inteligencia en relación con las ciberamenazas y las vulnerabilidades cibernéticas
- las medidas para una buena gestión por parte de las entidades financieras del **riesgo de terceros relacionado** con las TIC

b) Requisitos en relación con los **acuerdos contractuales celebrados entre proveedores terceros** de servicios de TIC **y entidades financieras**

c) El marco de **supervisión de los proveedores terceros esenciales** de servicios de TIC cuando presten servicios a entidades financieras

d) Normas sobre **cooperación entre autoridades competentes** y normas sobre supervisión y ejecución por parte de las autoridades competentes en relación con todos los asuntos cubiertos por el presente Reglamento

La aplicación de este **Reglamento** del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero, se ha previsto sobre un **principio de proporcionalidad** en el que para muchos de los requerimientos se tienen en cuenta las características específicas de las entidades

DORA asigna al órgano de dirección en un papel activo y central en la Dirección y adaptación del marco de gestión del riesgo de las TIC y de la estrategia en general

Órgano de Dirección

Es responsable de…

- Gestionar el riesgo relacionado con las TIC
- Definir y aprobar la estrategia de resiliencia operativa digital y un nivel adecuado de tolerancia al riesgo relacionado con las TIC
- Aplicar el marco de gestión del riesgo relacionado con las TIC
- Supervisar la exposición al riesgo de proveedores terceros de TIC y la documentación pertinente* (a través de un miembro del órgano de dirección**)

…debe definir, aprobar y revisar periódicamente…

- Marco de gestión del riesgo de las TIC Políticas garantizar niveles elevados de disponibilidad, autenticidad, integridad y confidencialidad de los datos
- Cometidos y responsabilidades y marco de comunicación, cooperación y coordinación de las funciones relacionadas con las TIC
- Política de continuidad, planes de respuesta y recuperación
- Planes e informes de auditoría interna de las TIC
- Política sobre acuerdos con proveedores de servicios de TIC

…debe habilitar…

- Una asignación presupuestaria adecuada para satisfacer las necesidades de resiliencia (programas de sensibilización en seguridad, formación en resiliencia y en capacidades de TIC para el personal)
- Canales de comunicación acerca de:
  - Acuerdos con proveedores terceros de TIC
  - Cambios relacionados con terceros de TIC
  - Repercusiones de tales cambios en las funciones esenciales y de las medidas de respuesta y recuperación

…debe disponer de…

- Capacidad suficiente para comprender y evaluar el riesgo relacionado con las TIC y sus repercusiones en las operaciones de la entidad
- Un plan de formación específica acorde con el riesgo relacionado con las TIC que gestione

* En entidades que no sean microempresas

** Alternativamente podrá crearse una función encargada de realizar un seguimiento de los acuerdos con proveedores terceros de TIC

La gestión del riesgo de terceros propuesta en DORA se basa en los siguientes principios generales

- Entidades financieras **responsables** en todo momento del cumplimiento del Reglamento.
- Aplicación con el **principio de proporcionalidad.**
- **Estrategia sobre el riesgo de terceros.**
- **Órgano de Dirección:** supervisión de estrategia y riesgos detectados en la operativa.
- **Registro de información** de acuerdos contractuales y a disposición de la autoridad competente.
- Comunicación a **autoridades competentes:**
  - Reporting ordinario anualmente.
  - Adhoc: Contratar funciones esenciales o importantes.
- Evaluación y requisitos de los **acuerdos contractuales.**
- **Auditoría** en terceros.
- Estrategias de **salida y continuidad** en los terceros.

} *Tratados más exhaustivamente durante el webinar*

En primer lugar, el Reglamento fija un marco de gobernanza de los riesgos proveedores de TIC, que se compone de una estrategia que debe contener ciertos requisitos mínimos, la cual aprueba y revisa el órgano de dirección

Estrategia que cubra cada uno de los proveedores de TIC a nivel de entidad

Dependencias clave de los proveedores	• Las dependencias clave de los proveedores terceros de servicios de TIC: (i) todos los procesos que dependan de proveedores terceros de servicios de TIC, y (ii) todas las interconexiones con proveedores terceros de servicios de TIC
Motivos para la contratación	• Explicación de los motivos subyacentes a la contratación de una combinación de proveedores terceros de servicios.
Política sobre el uso de servicios	• Una política sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC y se aplicará a nivel individual y, cuando proceda, en base subconsolidada y consolidada.
Inventarios de terceros	• Mantenimiento y actualización periódica de los inventarios de terceros pertinentes.
Planes de continuidad	• Planes de continuidad con proveedores terceros de servicios de TIC.

Responsabilidad del órgano de dirección:

- Las entidades no microempresas, deberán designar a **un miembro de la alta dirección como responsable de supervisar** la exposición al riesgo asociado a los acuerdos con terceros
- Aprobar y revisar periódicamente los **riesgos detectados por lo que respecta a la externalización** de funciones esenciales o importantes.
- Aprobar y revisar la **política de la entidad sobre los acuerdos relativos al uso de servicios de TIC** prestados por proveedores terceros de servicios de TIC.
- Será **debidamente informado** de:
  - Los **acuerdos celebrados** con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC,
  - cualquier **cambio sustancial pertinente** previsto en relación con los proveedores terceros de servicios de TIC,
  - del impacto **potencial de tales cambios en las funciones** esenciales o importantes sujetas a dichos acuerdos,
  - resumen del análisis de riesgos para evaluar el **impacto de los cambios**

DORA especifica requerimientos para la gestión y supervisión de riesgos con origen en la relación con terceros proveedores de TIC, según detallaremos en las siguientes páginas

Requerimientos de gobernanza del marco de gestión de riesgos TIC de terceros

Requerimientos a lo largo de los *Journeys* de relación con terceros proveedores TIC, como fuente de originación de riesgos TIC para la entidad

Evaluación previa – homologación de proveedores	Fase contractual	Monitorización del riesgo TIC de terceros	Estrategia de Salida y continuidad
• Se introducen requerimientos específicos sobre actuaciones que debe llevar a cabo la entidad, antes de **celebrar** un acuerdo contractual, en el marco de sus **procedimientos de homologación de terceros**	• Se introducen requerimientos concretos acerca del **contenido** que deben recoger los diferentes acuerdos contractuales con proveedores TIC terceros	• Se fijan requerimientos para la realización de **pruebas de resiliencia operativa** digital • Se fijan aspectos concretos sobre cómo abordar **auditorías de terceros** en ámbito de servicios TIC	• Se establecen requerimientos para las entidades en materia soluciones alternativas y **planes de transición**, que garanticen que el servicio no se perturba en caso de migración de proveedor

Y la supervisión de proveedores terceros esenciales

Alcance del cambio regulatorio

Supervisión de los proveedores terceros esenciales de servicios TIC

Supervisión de los proveedores terceros esenciales

- **Acto delegado por parte de la Comisión** Las AES designarán a los proveedores terceros de servicios de TIC que sean esenciales para las entidades financieras con criterios de esencialidad reforzada, y a los supervisores principales, ABE, la AEVM o la AESPJ (excepción Sistema Europeo de Bancos Centrales).

- Los **criterios de designación** de la esencialidad reforzada (art.31), entre otros, son relativos al efecto sistémico, dependencia, grado de sustituibilidad, el número de Estados a los que presta servicios y número de Estados en los que operan las entidades que recurren a ese proveedor.

- **Lista pública** que se actualizará anualmente. Los proveedores podrán solicitar a los supervisores voluntariamente su inclusión. 6 meses para resolver la solicitud.

- Las entidades no **podrán recurrir a un proveedor establecido en un Tercer país** que sería designado como esencial con arreglo a los criterios del art.31 si este no ha establecido una filial en la Unión en los 12 meses siguientes a la designación.

- **Facultades de supervisión**. Plan de supervisión anual comunicado al proveedor. Evaluación de cada proveedor (*solicitud de información, investigaciones generales o bien inspecciones in situ*) ha establecido todas las normas, procedimientos, mecanismos , etc. Necesarios para la gestión de riesgos TIC de las entidades (gestión de riesgos, SI, protección de datos, seguridad física, auditorías, infraestructuras, planes de contingencia, continuidad, portabilidad y respuesta).

- **Multa coercitiva diaria para obligar al proveedor**. 1% volumen de negocios diario medio a escala mundial

- **Tasas.** Las AES cobrarán a estos proveedores que cubran por completo los gastos de supervisión. Proporcional a su volumen de negocios.

Gracias

mvidal@finreg360.com

finReg360