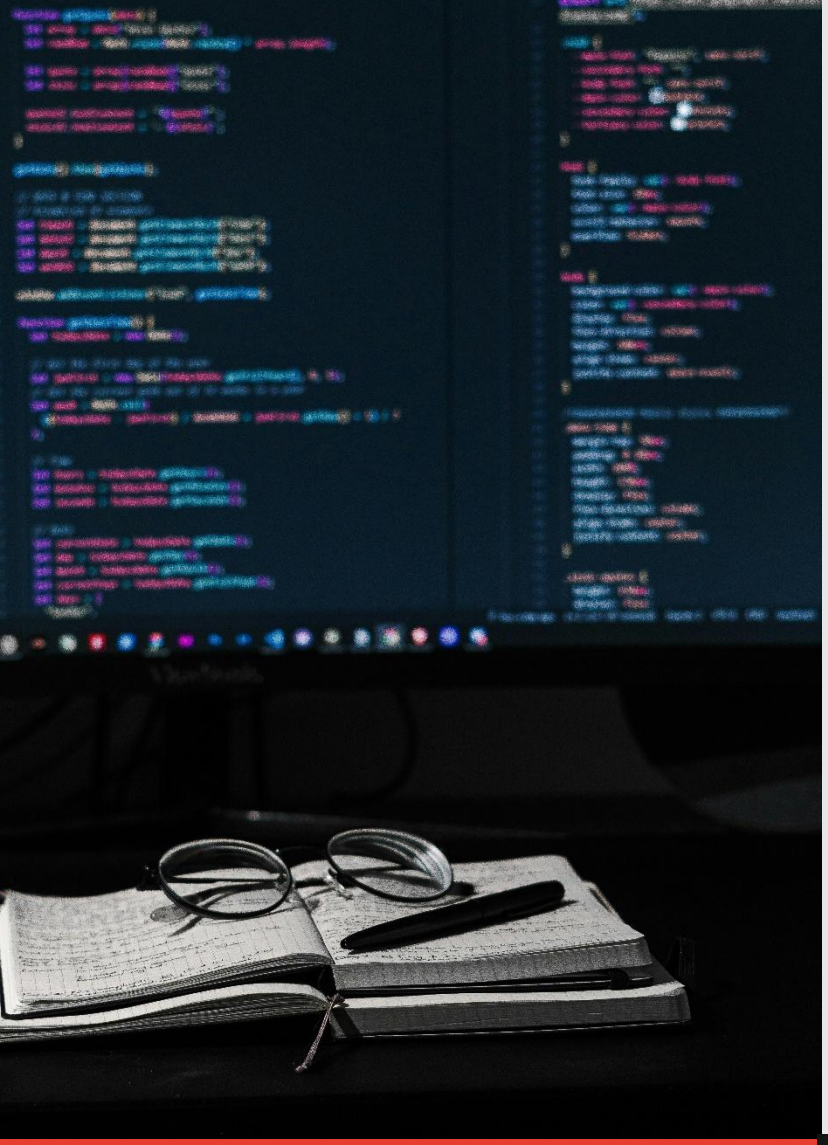

ECIJA

NOTA INFORMATIVA

Novedades en el cumplimiento de DORA

Análisis de las principales novedades con respecto al cumplimiento de las obligaciones del Reglamento DORA introducidas en el Anteproyecto de Ley de digitalización y modernización del sector financiero.

Uso público

Lo que necesitas saber

El Consejo de Ministros ha aprobado el anteproyecto de Ley de Digitalización y Modernización del Sector Financiero que tiene como objetivo, entre otros, garantizar en nuestro Ordenamiento Jurídico el cumplimiento de las obligaciones de ciberresiliencia del Reglamento 2022/2554 sobre la resiliencia operativa digital del sector financiero ("**DORA**").

En este ámbito, el borrador de ley incorpora las siguientes modificaciones:

- La **modificación de distintas normativas de carácter sectorial** del Ordenamiento Jurídico español para la implementación del régimen sancionador aplicable por incumplimientos del Reglamento DORA.

- El **establecimiento de los órganos con potestad de supervisión y sancionadora** para la imposición de las sanciones como consecuencia de las infracciones previstas.

- El **ajuste de las obligaciones de ciberresiliencia para operadores de sistemas de pagos, procesadores de pagos y esquemas de pagos**. Aunque estas entidades no están sujetas al Reglamento DORA, en España se decidió incluirlas en diciembre de 2023 para garantizar el buen funcionamiento del sistema de pagos.

La entrada en vigor del Reglamento DORA, a partir del **17 de enero de 2025**, supone que son aplicables sus obligaciones digiridas principalmente a las entidades financieras y aseguradoras.

No obstante, aunque el Reglamento es de aplicación directa, este no fija con precisión cuales serán las infracciones y sanciones aplicables, sino que se limita a indicar una serie de medidas que deberán ser impuestas por los Estados Miembros como sanciones administrativas o penales. En este sentido, resulta necesario el desarrollo normativo nacional para el establecimiento del régimen sancionador aplicable en el caso de incumplimientos de dichas obligaciones.

(I) Contexto normativo del Anteproyecto de Ley

El pasado 18 de diciembre el Consejo de Ministros ratificó el borrador de Ley de Digitalización y Modernización del Sector Financiero, cuyo propósito es **fomentar la innovación financiera** utilizando todas las posibilidades que ofrecen las tecnologías emergentes, asegurando simultáneamente un nivel de seguridad apropiado para las instituciones y los usuarios financieros. Este borrador de Ley se complementa con dos Reales Decretos que constituyen un conjunto de normativas integrales para la actualización del sector financiero.

Este conjunto de regulaciones incorpora a la legislación española diversas normativas y directrices comunitarias, y altera las regulaciones nacionales para promover la digitalización, impulsar la competencia y explotar las oportunidades que brinda el nuevo ambiente tecnológico, con un marco apropiado que minimice los riesgos, fomente la confianza de los usuarios y mantenga la estabilidad financiera.

El proyecto inicial se ha desarrollado en conjunto con el Banco de España, la CNMV y la Dirección General de Seguros y Fondos de Pensiones, además de otras entidades que tienen un interés directo en la digitalización del ámbito financiero.

(II) Principales infracciones

El régimen sancionador implementado en desarrollo del Reglamento DORA, parte de la definición de un conjunto homogéneo de infracciones, que, incorporadas a cada una de las normativas sectoriales, configuran el marco sancionador al que se expondrán las entidades sujetas a su ámbito de aplicación. Las infracciones de los siguientes preceptos son consideradas como **muy graves:**

- **Marco de gobernanza y organización**: incumplimiento del artículo 5 en caso de ausencia o grave deficiencia de un marco interno de gobernanza y control que garantice una gestión eficaz y prudente de todos los riesgos de las tecnologías digitales o de la información y la comunicación;
- **Marco de gestión del riesgo TIC**: incumplimiento del artículo 6 en caso de ausencia o grave deficiencia de un marco de gestión del riesgo sólido, completo y bien documentado;
- **Sistemas, protocolos y herramientas de TIC**: incumplimiento del artículo 7 en caso de mala utilización o falta de actualización que los haga inoperativos;
- **Identificación**: incumplimiento del artículo 8 en caso de falta de identificación, clasificación y documentación adecuada de todas las funciones empresariales relacionadas con las tecnologías digitales o de la

información y la comunicación, así como una falta de identificación de forma continua de todas las fuentes de riesgo derivadas de las tecnologías digitales o de la información y la comunicación;

- **Respaldo, reestablecimiento y recuperación**: incumplimiento del artículo 12 artículo 12 sobre las políticas y procedimientos de respaldo y procedimientos y métodos de restablecimiento y recuperación en caso de ausencia o grave deficiencia de dichas poilíticas y procedimientos;
- **Aprendizaje y evolución:** incumplimiento del artículo 13 sobre el aprendizaje y evolución en caso de ausencia o grave deficiencia de capacidades de personal y procesos para llevarlas a cabo;
- **Marco simplificado de gestión del riesgo TIC**: en su caso, cuando no exista dicho marco;
- **Gestión de ciberincidentes:** incumplimiento del artículo 18 sobre la clasificación de los incidentes relacionados con las TIC y las ciberamenazas en caso de ausencia de dicha clasificación ;
- **Notificación de ciberincidentes**: incumplimiento del artículo 19 sobre la notificación de los incidentes graves en caso de falta de notificación;
- **Pruebas de Resiliencia operativa digitial:** incumplimiento de los artículos 24, 25, 26 y 27 sobre la realización de pruebas de resiliencia operativa digital en caso de ausencia o grave deficiencia de pruebas adecuadas;
- **Gestión del riesgo derivado de terceros:** Incumplimiento del artículo 28 sobre los principios generales en la gestión de riesgo relacionado con las TIC derivado de terceros en caso de grave deficiencia o inobservancia de los principios establecidos en la gestión de riesgo cuando las entidades financieras celebran acuerdos con proveedores terceros de servicios TIC;
- **Evaluación preliminar del riesgo derivado de terceros:** incumplimiento del artículo 29 sobre la evaluación preliminar del riesgo de concentración TIC a nivel entidad en caso de ausencia o grave deficiencia de un proceso de evaluación previo para detectar elevadas dependencias de terceros y funciones esenciales que no deban ser subcontratadas;
- **Cláusulas contractuales con proveedores TIC:** Incumplimiento del artículo 30 sobre las cláusulas contractuales fundamentales en caso de ausencia o grave deficiencia de acuerdos contractuales sobre el uso de servicios TIC conforme a los requisitos que establece el artículo.

Por su parte, se considerarán **infracciones graves**, aquellas que con arreglo a los criterios anteriores no sean consideradas como muy graves, así como las siguientes:

- **Protección y prevención:** Incumplimiento del artículo artículo 9 en caso de falta de control continuo del funcionamiento de los sistemas y herramientas de tecnologías digitales o de la información y la comunicación;
- **Detección:** Incumplimiento del artículo artículo 10 en caso de ausencia de mecanismos para detectar rápidamente las actividades anómalas;
- **Respuesta y recuperación:** Incumplimiento del artículo 11 en caso de falta de una política de continuidad de las actividades de tecnologías digitales o de la información y la comunicación;
- **Comunicación:** Incumplimiento del artículo 14 en caso de falta de un plan de comunicación que permita la divulgación responsable de incidentes relacionados con las tecnologías digitales o de la información y la

comunicación o vulnerabilidades importantes a la clientela y contrapartes, así como al público, según proceda.

En último lugar, todas aquellas infracciones del Reglamento DORA no recogidas o que no tengan la entidad suficiente como para clasificarse en alguna de las anteriores categorías analizadas, y que afecten a los sujetos comprendidos en su ámbito de aplicación, tendrán la consideración de **infracciones leves**.

(III) Principales sanciones

El régimen sancionador implementado a través de las distintas modificaciones legislativas relacionadas en el apartado anterior **varía, en función del sector sobre el que opera**, e incorpora tanto sanciones de carácter pecuniario como una serie de sanciones y medidas correctoras establecidas en el artículo 50 DORA.

En cuanto a las sanciones de carácter pecuniario de las **infracciones muy graves aparejadas**, se observa que **la horquilla de multas se mueve entorno a los 5 y los 10 millones de euros**. A su vez, se imponen sanciones a los cargos de administración o directivos de las entidades sancionadas, que van desde las sanciones puramente pecuniarias, hasta sanciones de inhabilitación para el ejercicio del cargo por períodos de hasta 10 años. Las principales sanciones que incorpora el borrador de Ley en algunos de los sectores son las siguientes:

Fondos de pensiones, la potestad sancionadora es ejercida por la Dirección General de Seguros y Fondos de Pensiones. Se establecen las siguientes multas:

- Hasta 5.000.000 de euros o el 5% del volumen de negocios anual
- Hasta 1.000.000 de euros para cargos de administración o directivos
- Hasta 5.000.000 de euros para cargos de administración o directivos y/o inhabilitación para el ejercicio de su cargo de hasta 10 años.

Entidades de crédito, la potestad sancionadora es ejercida por el Banco de España. Se establecen las siguientes multas:

- Hasta 10.000.000 de euros o entre el 10% del volumen de negocios anual

Aseguradoras y reaseguradoras: la potestad sancionadora es ejercida por la Dirección General de Seguros y Fondos de Pensiones. Se establecen las siguientes multas:

- Hasta 5.000.000 de euros o el 5% del volumen de negocios anual
- Hasta 1.000.000 de euros para cargos de administración o directivos

Servicios de inversión: la potestad sancionadora es ejercida por la Comisión Nacional del Mercado de Valores. Se establecen las siguientes multas:

- Hasta 5.000.000 de euros o el 5% del volumen de negocios anual
- Hasta 1.000.000 de euros para cargos de administración o directivos y/o inhabilitación para el ejercicio de su cargo de hasta 10 años.

(IV) Ajuste de las obligaciones de ciertos sujetos en el marco de los servicios de pago

Por último, el borrador de Ley incorpora una modificación del texto del artículo 4 del Real Decreto-ley 8/2023, de 27 de diciembre, por el que se adoptan medidas para afrontar las consecuencias económicas y sociales derivadas de los conflictos en Ucrania y Oriente Próximo, así como para paliar los efectos de la sequía por el que se amplía en nuestro ordenamiento jurídico el ámbito de aplicación del Reglamento DORA a los **operadores de sistemas de pago, los operadores de esquemas de pago, los operadores de acuerdos de pago electrónico y los procesadores de pagos** que presten servicios en España y estén sujetos a supervisión o vigilancia por autoridades nacionales.

Aunque estas entidades no están sujetas al Reglamento DORA, en España se decidió incluirlas en diciembre de 2023 para garantizar el buen funcionamiento del sistema de pagos.

En concreto, se introduce el principio de proporcionalidad en el cumplimiento de las obligaciones del Capítulo II del Reglamento, y ahora también de la Sección I del Capítulo V, relativa a la gestión del riesgo de TIC derivado de terceros. Además se incorpora una mención expresa a la aplicabilidad del marco de gestión del riesgo TIC simplificado del artículo 16 a operadores de menor tamaño.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60