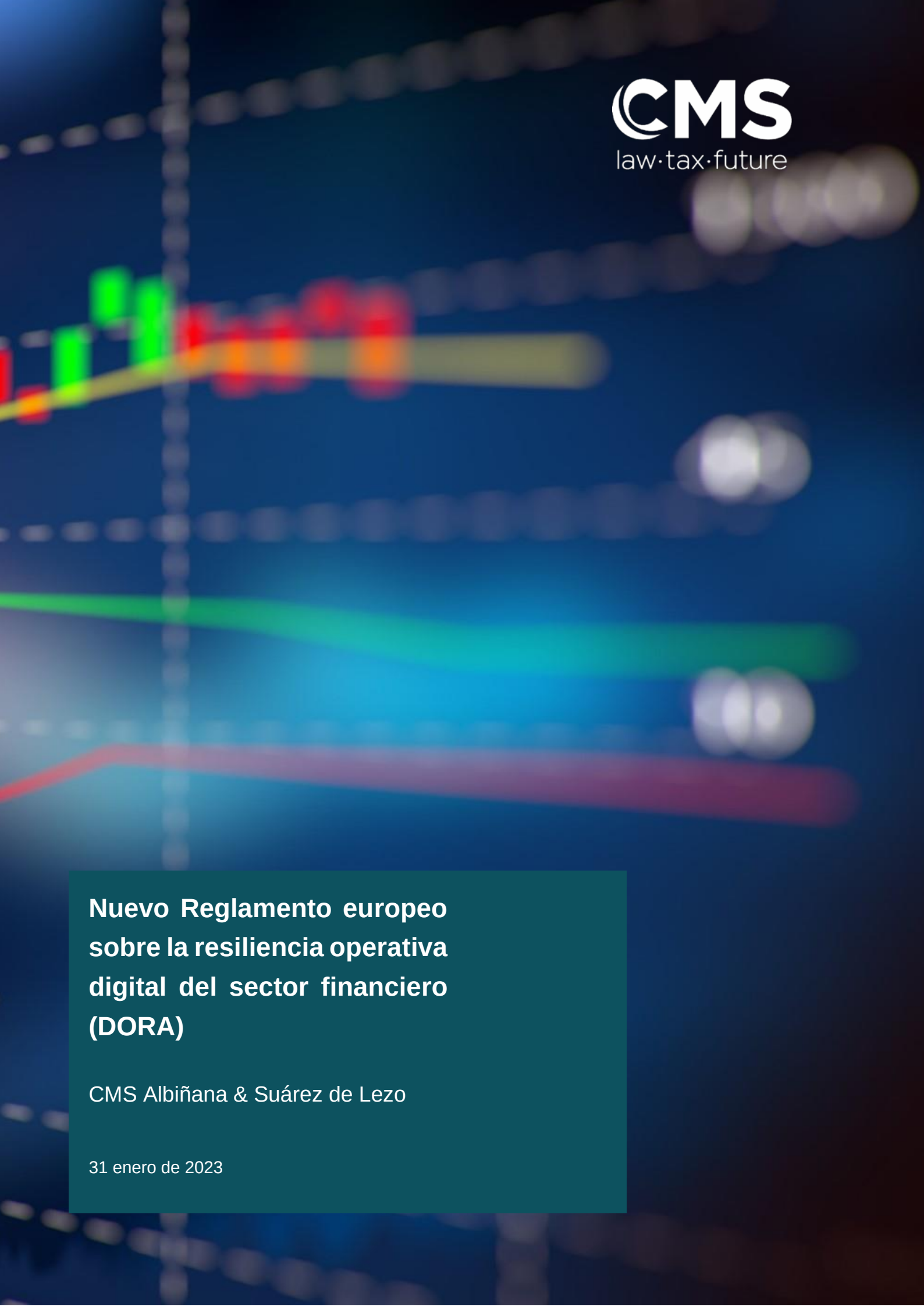

Nuevo Reglamento europeo sobre la resiliencia operativa digital del sector financiero (DORA)

CMS Albiñana & Suárez de Lezo

31 enero de 2023

NUEVO REGLAMENTO EUROPEO SOBRE LA RESILIENCIA OPERATIVA DIGITAL DEL SECTOR FINANCIERO (DORA)

El 27 de diciembre de 2022 se publicó en el Diario Oficial de la Unión Europea el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) 1060/2009, (UE) 648/2012, (UE) 600/2014, (UE) 909/2014 y (UE) 2016/1011 (el "**Reglamento**" o "**DORA**").

El Reglamento es simultáneo a la Directiva (UE) 2022/2556 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se modifican las Directivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 en lo relativo a la resiliencia operativa digital del sector financiero (la "**Directiva**").

Ambas disposiciones tienen el objetivo de lograr un elevado nivel común de resiliencia operativa digital, tal y como se define en el Reglamento y detallamos a continuación, estableciendo requisitos uniformes relativos a la seguridad de las redes y los sistemas de información que sustentan los procesos empresariales de las entidades financieras.

Los países de la Unión ya cuentan con normas en materia de riesgo operativo. Sin embargo, se han detectado lagunas a la hora de abordar dicho riesgo, de forma que se ha hecho necesaria una mayor precisión en cuanto a la protección, detección, contención, recuperación y reparación frente a incidentes relacionados con las tecnologías de la información y la comunicación ("**TIC**"), frente a las notificaciones de dichos riesgos o con respecto a las pruebas digitales que deben practicarse. El Reglamento colma dichas lagunas, estableciendo normas específicas sobre la gestión del riesgo, las notificaciones de incidentes, las pruebas de resiliencia operativa y el seguimiento del riesgo cuando éste deriva de terceros.

1. ÁMBITO DE APLICACIÓN Y OBJETO

Las entidades sujetas a la aplicación del Reglamento son, con determinadas exclusiones, todas las instituciones financieras. Así, queda vinculado un amplio abanico de sujetos: entidades de crédito, entidades de pagos, entidades de dinero electrónico, cualesquiera entidades de servicios de inversión, gestores de fondos de inversión alternativos, proveedores de servicios de criptoactivos, empresas e intermediarios de seguros y reaseguros, agencias de calificación crediticia, proveedores de servicios de financiación participativa o registros de titulizaciones, entre otros.

La gran novedad relacionada con el ámbito de aplicación del Reglamento es que también los llamados proveedores terceros de servicios de TIC pasan a estar bajo el área de vigilancia del Reglamento. Estos participantes son un gran apoyo para las entidades financieras en el sistema europeo y sus servicios actualmente son fundamentales para estas. De ahí que resulte primordial

evaluar y supervisar las normas, procedimientos y mecanismos con los que cuenten para gestionar sus riesgos TIC, así como sus consecuencias en las entidades financieras. Del Reglamento se desprende que un riesgo TIC es "*cualquier circunstancia razonablemente identificable en relación con el uso de redes y sistemas de información que, si se materializa, puede comprometer la seguridad de las redes y sistemas de información, de cualquier herramienta o proceso dependiente de la tecnología, de las operaciones y los procesos o de la prestación de servicios, al provocar efectos adversos en el entorno digital o físico*".

El objetivo principal del Reglamento, como se ha indicado, es logar un nivel adecuado de resiliencia operativa digital común al conjunto de los Estados miembros de la Unión Europea. De acuerdo con el texto de DORA, se entiende por resiliencia operativa digital "*la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones*".

El Reglamento marca las reglas en diversos aspectos de los procesos de las entidades que se encuentran bajo su ámbito de aplicación y, en concreto, fija los requisitos aplicables a entidades financieras y los requisitos en relación con los acuerdos contractuales entre proveedores terceros de servicios de TIC y entidades financieras. Además, regula el establecimiento y aplicación del marco de supervisión de los proveedores terceros esenciales de servicios de TIC cuando prestan servicios a entidades financieras.

2. REQUISITOS APLICABLES A ENTIDADES FINANCIERAS

En primer lugar, de cara a favorecer la gestión del riesgo relacionado con las TIC, se impulsa la creación de un marco sólido, rápido, eficiente y exhaustivo que asegure un nivel alto de resiliencia operativa digital. Dicho marco deberá incluir todos aquellos procedimientos o herramientas necesarios para la debida protección de los activos de información y activos TIC (es decir, software, hardware, o servidores, así como centros de datos o infraestructuras físicas). Entre otros, las entidades financieras deberán llevar un seguimiento y control permanente de la seguridad y funcionamiento de los sistemas y herramientas, dispondrán de mecanismos de detección rápida de actividades anómalas y aplicarán la política de continuidad de la actividad en cuanto a TIC para garantizar la continuidad de actividades esenciales de la entidad financiera.

Por otra parte, las entidades financieras llevarán un registro de los incidentes relacionados con las TIC o ciberamenazas importantes clasificándolas y fijando su repercusión, con las indicaciones pertinentes en relación con la información exigida por el Reglamento. Lo anterior será de aplicación para los incidentes operativos o de seguridad relacionados con pagos cuando involucren a entidades de crédito, de pago, proveedores de servicios de información sobre cuentas

y entidades de dinero electrónico. Asimismo, las entidades deberán notificar los incidentes considerados graves a la autoridad competente que proceda. Las obligaciones de información podrán externalizarse a proveedores terceros de servicios.

Para evaluar el nivel de resiliencia operativa digital de las entidades financieras, aquellas que no sean microempresas establecerán, mantendrán y revisarán un programa de pruebas sólido y completo que forme parte del marco de gestión del riesgo relacionado con las TIC. El programa debe considerar todo riesgo especifico al que la entidad esté o pueda estar expuesta y cualquier factor que se considere apropiado. Determinadas entidades, debido a su gran tamaño y al posible impacto de defectos o errores en sus sistemas, llevarán a cabo pruebas avanzadas consistentes en pruebas de penetración basadas en amenazas, al menos con una regularidad de tres años, a través de probadores que cuenten con un nivel adecuado de idoneidad, capacidades y conocimientos, acreditación y garantías, según dispone el Reglamento.

El Reglamento prevé asimismo la posibilidad de que las entidades puedan intercambiar información e inteligencia en relación con las ciberamenazas y las vulnerabilidades relacionadas, cuando dicho intercambio favorezca la mejora de la resiliencia operativa digital, este tenga lugar dentro de comunidades de entidades de confianza, y existan acuerdos que protejan dichos intercambios, el secreto comercial, los datos personales, y las políticas de competencia. Estos intercambios permiten que el sector financiero responda colectivamente a las amenazas, limitando su propagación e impidiendo el efecto contagio a través de los canales financieros.

3. REQUISITOS EN RELACION CON LOS ACUERDOS CONTRACTUALES ENTRE PROVEEDORES TERCEROS DE SERVICIOS DE TIC Y ENTIDADES FINANCIERAS

Uno de los puntos más importantes que introduce el Reglamento son las medidas para la buena gestión del riesgo relacionado con las TIC derivado de terceros, en particular cuando las entidades financieras recurren a proveedores terceros de servicios TIC para sustentar funciones esenciales o importantes de su actividad. Se entiende por función esencial o importante aquella "*cuya perturbación afectaría significativamente al rendimiento financiero de una entidad financiera o a la solidez o continuidad de sus servicios y actividades o cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización*".

A pesar de la existencia de las Directrices de la Autoridad Bancaria Europea (EBA) de 2019 sobre externalización y las Directrices de la Autoridad Europea de Mercados de Valores (ESMA) de 2021 sobre externalización de servicios a proveedores de servicios en la nube, el derecho de la Unión no aborda de manera suficiente la gestión del riesgo sistémico que puede desencadenarse en el sector financiero con la entrada de proveedores terceros de servicios de TIC, ni permite comprender o hacer un seguimiento adecuado de dichos riesgos relacionados con las TIC.

Para ello, será esencial que la relación entre la entidad y el tercero esté debidamente recogida en un contrato por escrito, que contenga los derechos y obligaciones de ambas partes de forma duradera y accesible. Se trata, con ello, de salvaguardar mínimamente dicha relación y hacer seguimiento por parte de las entidades financieras de todos los riesgos relacionados con las TIC que puedan surgir por el lado de los proveedores. Como apunta el Reglamento, estas exigencias serán complementarias al derecho sectorial aplicable a la externalización.

El Reglamento determina aquellas cuestiones que, independientemente de si la función fuese considerada o no como esencial o importante, deben recoger los contratos entre las entidades financieras y los proveedores terceros de servicios de TIC. En caso de que las funciones sean consideradas como esenciales o importantes, las exigencias contractuales que fija el Reglamento son mayores.

4. ESTABLECIMIENTO Y APLICACIÓN DEL MARCO DE SUPERVISION DE LOS PROVEEDORES TERCEROS ESENCIALES DE SERVICIOS DE TIC CUANDO PRESTAN SERVICIOS A ENTIDADES FINANCIERAS

Por último, se establece un marco de supervisión de los proveedores terceros esenciales de servicios de TIC que permita hacer un seguimiento continuo de sus actividades, favoreciendo que la prestación de servicios TIC por proveedores ajenos esté sujeta al mismo marco normativo que en caso de prestarse de forma interna por la entidad financiera.

Las Autoridades Europeas de Supervisión, a través del Comité Mixto y por recomendación del Foro de Supervisión, designarán a los proveedores terceros esenciales de servicios de TIC cuando prestan servicios a entidades financieras, tras la debida evaluación. Dicha evaluación tendrá en cuenta, a rasgos generales:

(i) el impacto sistémico en la estabilidad, la continuidad o la calidad de la prestación de servicios financieros en caso de un posible fallo operativo a gran escala del proveedor que afecte a la prestación de sus servicios;

(ii) el carácter o la importancia sistémicos de las entidades financieras que dependen del proveedor, evaluados con arreglo al número de entidades de importancia sistémica mundial u otras entidades de importancia sistémica que dependen del proveedor, y a la interdependencia entre las mencionadas entidades y otras entidades financieras;

(iii) la dependencia de las entidades financieras respecto de los servicios prestados por el proveedor en relación con funciones esenciales o importantes que, en última instancia, impliquen al mismo proveedor, con independencia de que las entidades financieras recurran a dichos servicios directa o indirectamente, a través de acuerdos de subcontratación; y

(iv) el grado de sustituibilidad del proveedor, teniendo en cuenta la falta de alternativas reales o las dificultades relacionadas con la migración parcial o total de los datos y cargas de trabajo pertinentes del proveedor en cuestión a otro.

Asimismo, deberán nombrar a la Autoridad Europea de Supervisión pertinente como supervisor principal de cada proveedor tercero esencial de servicios de TIC.

5. ENTRADA EN VIGOR Y APLICACIÓN

El Reglamento DORA y la Directiva han entrado en vigor el 17 de enero de 2023, y el Reglamento DORA será aplicable de forma directa a partir del 17 de enero de 2025.

Ricardo Plasencia
Socio CMS
Mercados y Servicios Financieros
T +34 91 187 19 13
E ricardo.plasencia@cms-asl.com

Lucía Escauriaza
Asociada CMS
Mercados y Servicios Financieros
T +34 91 451 93 35
E lucia.escauriaza@cms-asl.com