Actualidad Jurídica Uría Menéndez, 67, mayo 2025, pp. 255-262

Foro de Actualidad

Unión Europea

REGLAMENTO DORA: UN CAMBIO DE PARADIGMA EN LAS OBLIGACIONES DE CIBERSEGURIDAD DEL SECTOR FINANCIERO

Juan Sebastián Gómez Castro y Martín Montilla Castilla

Abogados de Phillipi, Prietocarrizosa Ferrero DU & Uría y del Área de Mercantil de Uría Menéndez, respectivamente (Colombia y Madrid)

Reglamento DORA: un cambio de paradigma en las obligaciones de ciberseguridad del sector financiero

En este foro se analizan las obligaciones del Reglamento de Resiliencia Operativa Digital (conocido como "Reglamento DORA") tanto para las entidades financieras como para sus proveedores de servicios TIC tras su entrada en aplicación el pasado 17 de enero de 2025. El Reglamento DORA supone un cambio de paradigma para la regulación de la ciberseguridad de las entidades financieras, ya que, por primera vez, los prestadores de servicios tecnológicos entran dentro de su ámbito subjetivo.

PALABRAS CLAVE:
Reglamento DORA, Entidades financieras, Proveedores de servicios de TIC, Ciberseguridad, Ciberresiliencia.

DORA Regulation: a paradigm shift in cybersecurity obligations for the financial sector

This article analyses the obligations of the Digital Operational Resilience Act (known as "DORA") for both financial institutions and their ICT service providers after it came into force on 17 January 2025. DORA represents a major change in how cybersecurity is regulated for financial entities, as it now includes technology service providers for the first time.

KEYWORDS:
DORA, financial institutions, ICT service providers, cybersecurity, cyber-resilience.

FECHA DE RECEPCIÓN: 24-3-2025

FECHA DE ACEPTACIÓN: 31-3-2025

Gómez Castro; Juan Sebastián; Montilla Castilla, Martín (2025). Reglamento DORA: un cambio de paradigma en las obligaciones de ciberseguridad del sector financiero. *Actualidad Jurídica Uría Menéndez*, 67, pp. 255-262 (ISSN: 1578-956X).

1. Introducción: contexto del Reglamento DORA

Entre las normas que pretenden asegurar un nivel adecuado de ciberseguridad en todo el mercado interior se encuentra 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 ("Reglamento DORA", por sus siglas en inglés), que es de aplicación al sector financiero (que comprende de manera amplia a banca, mercado de valores y seguros). Tras su publicación en el *Diario Oficial de la UE* el 27 de diciembre de 2022, el 17 de enero de 2025 todas las disposiciones del Reglamento DORA comenzaron a tener aplicación, por lo que las entidades financieras (y sus proveedores) se encuentran actualmente sometidos a esta normativa.

El Reglamento DORA pretende lograr un elevado nivel común de resiliencia operativa digital en el mercado interior de la Unión Europea para las entidades del sector financiero. Para ello, establece unos requisitos uniformes relativos a la seguridad de las redes y los sistemas de información de las entidades financieras que sustentan sus procesos empresariales.

Además, un punto relevante del Reglamento DORA es que, por primera vez, los prestadores de servicios de las tecnologías de la información y la comunicación ("proveedores de servicios de TIC") también entran dentro del ámbito de aplicación de la norma y, por tanto, sus disposiciones les son directamente aplicables. Hasta ahora, estos proveedores estaban obligados a cumplir con ciertas obligaciones de seguridad en sus relaciones con las entidades financieras en la medida en que los contratos con estas entidades debían contener un contenido de ciberseguridad obligatorio. Sin embargo, la aplicación del Reglamento DORA supone que ciertas obligaciones sean de aplicación directa a estos proveedores, sin depender únicamente del contrato suscrito.

2. Ámbitos de aplicación: objetivo y subjetivo

Para alcanzar unos niveles elevados de resiliencia operativa digital de las entidades financieras, el Reglamento DORA contempla múltiples reglas en relación con la seguridad de las redes y los sistemas de información que utilizan las entidades financieras en sus procesos operativos. De manera general, estas disposiciones normativas pueden agruparse en cuatro categorías: (i) requisitos aplicables a las entidades financieras en relación con la gestión del riesgo de TIC, la notificación de incidentes graves relacionados con las TIC, y las pruebas de resiliencia, entre otros; (ii) requisitos mínimos para los acuerdos contractuales celebrados entre entidades financieras y proveedores de servicios de TIC; (iii) marco de supervisión de los proveedores terceros esenciales de servicios de

TIC; y (iv) normas sobre cooperación entre autoridades competentes, intercambio de información e inteligencia, así como disposiciones sancionatorias, de control y ejecución.

Desde un punto de vista subjetivo, el Reglamento DORA es aplicable a dos tipos de sujetos: *entidades financieras*, dentro de las cuales se incluyen, por ejemplo, entidades de crédito, entidades de pago, entidades de dinero electrónico, empresas de servicios de inversión y depositarios centrales de valores, y se excluyen otras como intermediarios de seguros, reaseguros y de seguros complementarios que sean microempresas o pequeñas o medianas empresas; y *proveedores terceros de servicios de TIC*, los cuales se definen en el Reglamento DORA como empresas que prestan "*servicios digitales y de datos* (...) *a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua*".

No obstante, la mayor parte del Reglamento DORA está dirigido a entidades financieras, a las que se les establecen obligaciones para garantizar y asegurar la integridad y fiabilidad de las redes y los sistemas de información que sustentan la operación y prestación efectiva de sus servicios. La manera en que están escritas estas normas —artículos 4 a 27 del Reglamento DORA— evidencia sin duda alguna que sus destinatarios son exclusivamente las entidades financieras: "*las entidades financieras deberán* (...) *establecerán* (...) *minimizarán* (...) *utilizarán y mantendrán* (...) *aplicarán* (...) *crearán*".

Por el contrario, el artículo 30 del Reglamento DORA trae un enfoque normativo diferente al de las disposiciones que lo anteceden, pues no contempla obligaciones directas a los sujetos obligados, sino que establece que los derechos y obligaciones de la entidad financiera y del proveedor de servicios de TIC, en relación con los acuerdos para el uso de servicios de TIC, deberán constar en un contrato por escrito. Así, su redacción impone un contenido mínimo fundamental en este tipo de contratos y no obligaciones específicas a estos sujetos. En esta línea, el artículo 30.2 establece que "*Los acuerdos contractuales sobre el uso de servicios de TIC incluirán, como mínimo, los elementos siguientes:* (...)". En consecuencia, esta es una norma que se limita a fijar requisitos mínimos que deben contener los contratos entre entidades financieras y sus proveedores de servicios de TIC.

3. Principales obligaciones del Reglamento DORA

3.1. Obligaciones para las entidades financieras

El principal foco de las obligaciones contempladas en el Reglamento DORA va dirigido a las entidades financieras, ya que el propósito de la norma es precisamente asegurar un adecuado nivel de seguridad en sus redes y sistemas de información. Así, el Reglamento DORA impone a las entidades financieras distintas obligaciones en materia de seguridad que tienen incidencia directa en su estructura interna.

El Reglamento DORA establece obligaciones de gobernanza de la seguridad a las entidades financieras, de manera que sus órganos de dirección deben definir un marco de gestión del riesgo e implementar las medidas que se consideren adecuadas para prevenir los riesgos relacionados

con las TIC. Este marco de gestión deberá incluir las estrategias, las políticas, los procedimientos, y los protocolos y herramientas de TIC que sean necesarios para proteger debida y adecuadamente todos los activos de información y activos de TIC. Además, el artículo 5.2 del Reglamento DORA contempla la responsabilidad última del órgano de dirección de la entidad financiera en el cumplimiento de estas obligaciones.

Otro punto fundamental del Reglamento DORA es el relativo a la detección, notificación y mitigación de incidentes de seguridad. Las entidades financieras deben instaurar procesos de detección de incidentes de seguridad relacionados con las TIC y, en caso de que se detecte algún incidente, llevar a cabo un proceso de clasificación. Si el incidente alcanzara la consideración de "grave", entonces se activa la obligación de comunicarlo a la autoridad competente, sin perjuicio de que también se puedan notificar incidentes de menor importancia.

Otra obligación relevante para las entidades financieras es que deben realizar, con cierta periodicidad, pruebas de resiliencia operativa digital para comprobar que las medidas de seguridad adoptadas son suficientes para prevenir los riesgos asociados con las TIC. Así, las entidades financieras deberán realizar pruebas de penetración basadas en amenazas, que son una suerte de "simulacros" que replican ciberamenazas a las que se pueden enfrentar las entidades financieras y así comprobar que el marco de gestión del riesgo de las TIC es adecuado.

Aunque las obligaciones impuestas en el Reglamento DORA son extensas y conllevan una alta complejidad técnica, el artículo 4 del Reglamento DORA introduce un *principio de proporcionalidad*, que pretende adaptar el cumplimiento de estas obligaciones en virtud del tamaño de la entidad y el perfil de riesgo general (así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones). Con esto se pretende adecuar la intensidad de las obligaciones de esta norma a la naturaleza y tamaño de la entidad financiera.

3.2. Principios para la gestión del riesgo relacionado con las TIC derivado de terceros

Otro de los objetivos principales del Reglamento DORA es que las entidades financieras no solo gestionen adecuadamente los riesgos en materia de TIC desde el punto de vista de su organización, sino que también tengan en cuenta los riesgos que se puedan derivar de terceros. Para administrar los riesgos que puedan emanar al contratar con un tercero la prestación de un servicio de TIC, el Reglamento DORA se fundamenta en una serie de principios y criterios que orientan la contratación de estos servicios. Así, el artículo 28.1.b) del Reglamento DORA dispone que las entidades financieras, al gestionar dicho riesgo de acuerdo con el principio de proporcionalidad, también tendrán que considerar factores como (i) la naturaleza, escala, complejidad e importancia de las dependencias en relación con las TIC; (ii) el carácter esencial o la importancia del servicio de TIC contratado; (iii) el proceso o la función particular de que se trate; y (iv) el potencial efecto del servicio de TIC en la continuidad y disponibilidad de los servicios de la entidad financiera.

En segundo lugar, el Reglamento DORA señala que las entidades financieras deberán realizar una evaluación exhaustiva del riesgo antes de celebrar un contrato para el uso de servicios de TIC. En este análisis previo, las entidades financieras tienen que evaluar, por ejemplo, si los servicios de

TIC a contratar sustentan una función esencial o importante, si dicho acuerdo puede reforzar el riesgo de concentrar servicios de TIC en un proveedor difícilmente sustituible, la coexistencia de varios acuerdos contractuales que sustenten funciones esenciales o importantes con el mismo proveedor, o la idoneidad suficiente del proveedor correspondiente.

En tercer lugar, el Reglamento DORA solo permite que las entidades financieras celebren acuerdos contractuales con proveedores terceros de servicios de TIC que cumplan estándares adecuados en materia de seguridad de la información. Asimismo, precisa que las entidades financieras deben tener garantizada la posibilidad de terminar los acuerdos contractuales sobre el uso de servicios de TIC cuando (i) se presente un incumplimiento importante por parte del proveedor; (ii) ocurran circunstancias sobrevenidas que puedan alterar el desempeño de los servicios prestados; o (iii) aparezcan debilidades manifiestas del proveedor de servicios de TIC en cuanto a su gestión global del riesgo relacionado con las TIC.

Finalmente, el Reglamento DORA dispone que, en los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes, las entidades financieras deben tener estrategias de salida de los contratos, asegurándose, particularmente, que puedan abandonar los contratos sin perturbar sus operaciones comerciales o limitar el cumplimento de los requisitos reglamentarios, así como no perjudicar la continuidad y la calidad de los servicios prestados a sus clientes.

3.3. Contenido mínimo de los contratos entre las entidades financieras y sus proveedores de servicios de TIC

Como se mencionó anteriormente, el Reglamento DORA consagra una serie de cláusulas fundamentales que deben estar en todos los contratos que celebre una entidad financiera con un proveedor de servicios de TIC. Particularmente, su artículo 30.2 establece un contenido mínimo aplicable a todos estos acuerdos, independientemente de que el servicio contratado sustente o no una función esencial o importante de la entidad financiera. Este clausulado mínimo consiste en (i) una descripción clara y completa de todas las funciones y servicios de TIC a prestar; (ii) la definición de las regiones o países en los que deberán prestarse los servicios de TIC, incluyendo el lugar de tratamiento y almacenamiento de los datos correspondientes; (iii) disposiciones sobre la disponibilidad, autenticidad, integridad y confidencialidad de los datos, incluidos los datos personales; (iv) reglas para garantizar que, en caso de insolvencia o interrupción de las actividades comerciales del proveedor o de terminación del acuerdo contractual, la entidad financiera pueda acceder, recuperar y recibir todos los datos que hayan sido objeto de tratamiento; (v) la descripción del nivel de servicio; (vi) la obligación del proveedor de ayudar a la entidad financiera cuando se produzca un incidente de TIC, sin coste adicional o a un coste determinado con anterioridad; (vii) la obligación de cooperar con las autoridades de supervisión de la entidad financiera; (viii) derechos de terminación a favor de la entidad financiera y los plazos mínimos de notificación para la terminación de los acuerdos contractuales; y (ix) la obligación de participar en los programas de sensibilización y formación sobre seguridad de las TIC y resiliencia operativa digital de las entidades financieras.

Adicionalmente, si la entidad financiera determina previamente que el servicio de TIC a contratar con el proveedor correspondiente sustenta funciones esenciales o importantes en relación con su actividad, los acuerdos contractuales deberán incluir el siguiente contenido adicional: (i) descripciones completas del nivel de servicio, con objetivos de rendimiento cuantitativos, cualitativos y precisos, de tal forma que se pueda hacer seguimiento efectivo al proveedor y adoptar medidas correctivas cuando corresponda; (ii) la obligación del proveedor de informar a la entidad financiera cualquier hecho que pueda afectar considerablemente su capacidad de prestar los servicios según los niveles de acordados; (iii) la obligación del proveedor de implementar y poner a prueba planes de contingencia empresarial y disponer de medidas, herramientas y políticas de seguridad de las TIC que proporcionen un nivel adecuado de seguridad para la prestación de los servicios; (iv) la obligación del proveedor de participar y cooperar en las pruebas de penetración basadas en amenazas de la entidad financiera; (v) derechos ilimitados a favor de la entidad financiera, y de su autoridad supervisora, para acceder, inspeccionar y auditar al proveedor; y (vi) estrategias de salida que incluyan un período de transición suficiente durante el cual se garantice que el proveedor continuará prestando sus servicios y se permita la migración necesaria.

En resumen, el Reglamento DORA establece dos niveles de contenido mínimo contractual: uno básico que resulta aplicable a todos los contratos con proveedores de servicios de TIC y otro adicional que solo es aplicable a los contratos para la prestación de servicios de TIC que sustenten funciones esenciales o importantes.

3.4. Marco de supervisión de los proveedores terceros esenciales de servicios de TIC

La principal novedad del Reglamento DORA respecto de otras normas en materia de ciberseguridad es que establece un régimen de supervisión directa de determinados proveedores de servicios de TIC que tengan una especial relevancia en el mercado.

A estos efectos, las autoridades de supervisión (es decir, la Autoridad Bancaria Europea, la Autoridad Europea de Seguros y Pensiones de Jubilación y la Autoridad Europea de Valores y Mercados) deben realizar una evaluación de los proveedores de servicios de TIC de las entidades financieras teniendo en cuenta los criterios establecidos en el artículo 31.2 del Reglamento DORA y, tras esta revisión, designar a los proveedores terceros esenciales de servicios de TIC. Algunos de estos criterios son los siguientes: (i) posible impacto sistémico en la estabilidad, continuidad o calidad de la prestación de los servicios financieros en caso de un fallo operativo a gran escala del proveedor de servicios de TIC; (ii) importancia sistémica de las entidades financieras que dependen del proveedor de servicios de TIC correspondiente; o (iii) nivel de sustituibilidad del proveedor de servicios de TIC.

A los proveedores terceros esenciales de servicios de TIC les será de aplicación el marco de supervisión establecido en la sección II del capítulo V del Reglamento DORA, ya que se entiende que, por su relevancia en el mercado, un incidente de seguridad puede tener una especial afectación en el sector financiero en su conjunto.

Esta supervisión conlleva una evaluación que realizará el supervisor principal sobre si los proveedores terceros esenciales han establecido normas y procedimientos para gestionar el riesgo

relacionado con las TIC que puedan plantearse a las entidades financieras. Esta evaluación abarca, entre otros aspectos, (i) los requisitos para garantizar la seguridad, disponibilidad, continuidad, escalabilidad y calidad de los servicios; (ii) la seguridad física del proveedor; (iii) los procesos de gestión de riesgos; (iv) los mecanismos de gobernanza; (v) la determinación, seguimiento y rápida notificación a las entidades financieras de los incidentes importantes relacionados con las TIC; y (vi) las auditorías de TIC. Sobre la base de esta evaluación, el supervisor principal adoptará un plan de supervisión para cada proveedor tercero esencial.

Adicionalmente, en el ejercicio de sus facultades de supervisión, el supervisor principal podrá solicitar toda la información y documentación pertinente para realizar su supervisión, llevar a cabo investigaciones generales e inspecciones, formular recomendaciones y solicitar informes en los que se especifiquen las medidas adoptadas en relación con las recomendaciones aportadas. Con el fin de que el proveedor tercero esencial cumpla con las recomendaciones y medidas exigidas por el supervisor principal, este podrá imponer multas administrativas coercitivas con el fin de asegurar su cumplimiento.

Finalmente, la designación como proveedor tercero esencial de servicios de TIC también conlleva la obligación de sufragar, mediante el pago de tasas, los costes en los que incurra el supervisor principal para ejercer sus facultades de supervisión.

4. Desarrollo futuro del Reglamento DORA

Debe destacarse que la regulación de la resiliencia operativa digital de las entidades financieras no se detiene en el Reglamento DORA. La variedad y complejidad de las disposiciones previstas en esta norma están complementadas y detalladas en numerosos actos delegados y de ejecución técnica que fijan de manera precisa la forma en que los sujetos obligados deben cumplir sus obligaciones. A fecha de este artículo, existen diez actos delegados, complementarios del Reglamento DORA, publicados en el *Diario Oficial de la UE*.

En efecto, encontramos, por ejemplo, reglamentos delegados y de ejecución que especifican los criterios para la clasificación de los incidentes relacionados con las TIC y las ciberamenazas; que fijan el contenido de la política relativa a los acuerdos contractuales que deben tener las entidades financieras sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes; que precisan el contenido y los plazos para la notificación de incidentes graves relacionados con las TIC; o que determinan los criterios para la designación de proveedores terceros esenciales de servicios de TIC. De igual manera, se espera la aprobación de otros actos delegados que regulen, entre otras cuestiones, los elementos que una entidad financiera debe determinar y analizar al subcontratar servicios de TIC que sustenten funciones esenciales o importantes, o los criterios técnicos que deben utilizar las entidades financieras para realizar las pruebas de penetración basadas en amenazas.

Adicionalmente, en lo relativo a la negociación de los aspectos contractuales con mayores implicaciones prácticas —como pueden ser los derechos ilimitados de acceso, inspección, auditoría o las pruebas de penetración basadas en amenazas— no debe descartarse que las entidades financieras y sus proveedores de servicios de TIC adopten criterios o prácticas poco comunes en la actualidad, pero que se terminen convirtiendo en estándares de mercado.

Además, para asegurar su cumplimiento, el Reglamento DORA también establece que los Estados miembros de la UE deben conferir a las autoridades competentes la facultad para imponer sanciones administrativas o medidas correctoras. En España, el régimen sancionador por incumplimientos del Reglamento DORA se quiere establecer, de manera general, a través del actual Anteproyecto de Ley de digitalización y modernización del sector financiero. De acuerdo con su exposición de motivos, este anteproyecto busca establecer el régimen sancionador común al sector financiero por infracciones del Reglamento DORA, para lo cual contempla la modificación de diversas normas. Sin embargo, a fecha de este artículo no se ha aprobado el texto definitivo y, por lo tanto, aún queda pendiente conocer cómo se implementará finalmente este régimen sancionador en España.

El artículo 52 del Reglamento DORA también abre la puerta a que los Estados miembros establezcan sanciones penales a los sujetos obligados por su incumplimiento, lo que supone una novedad relevante. Sin embargo, a fecha de hoy parece que el legislador español no pretende establecer sanciones penales específicas por incumplimientos de esta normativa.

5. Conclusiones

La plena aplicación del Reglamento DORA supone un cambio en las obligaciones de resiliencia operativa de las entidades financieras y, en particular, en cuanto a las relaciones con sus proveedores de servicios de TIC. Así, las entidades financieras no solo tendrán que analizar internamente los riesgos relacionados con el uso de las TIC e implementar medidas adecuadas al riesgo, sino que también deben prestar especial atención a la capacidad de sus proveedores de servicios de TIC de asegurar esta seguridad frente a los riesgos identificados. Con este fin, el Reglamento DORA obliga a que los contratos entre entidades financieras y proveedores de servicios de TIC tengan un cierto contenido obligatorio. Lo anterior, naturalmente, implica que las partes de dichos contratos deberán ser cuidadosas en la negociación de los contratos para no obviar el contenido imperativo de la norma.

Pero el Reglamento DORA también establece un marco de supervisión específico para aquellos proveedores de servicios de TIC que sean considerados como esenciales, de manera que un incidente de seguridad en estos proveedores implique una grave afectación a las funciones esenciales o importantes de las entidades financieras. Así, se produce un cambio de paradigma al incluir directamente a estos proveedores en el ámbito subjetivo del Reglamento DORA.

El gran volumen de obligaciones que contempla la norma, la necesidad de desarrollar algunas de sus disposiciones a través de actos delegados o normativa nacional y la complejidad de la negociación de los contratos entre entidades financieras y proveedores con el fin de cumplir con la normativa supone un gran desafío de cara a los próximos años en materia de resiliencia operativa de las entidades financieras. Por tanto, todos los sujetos implicados deben estar preparados para comprender y enfrentar no solo las disposiciones que introduce el Reglamento DORA, sino también todo el nuevo derecho que surgirá de su aplicación práctica.