

NORMA UE · SECTOR FINANCIERO

DORA: cuando su cliente es un banco de la UE

Desde el 17/01/2025, los bancos, las aseguradoras y otras entidades financieras de la UE deben seleccionar, contratar y supervisar a sus proveedores de TI según reglas fijas. Quien les entrega software, servicios de centro de datos o soporte de TI lo nota de inmediato.

FUENTE LEGAL	VIGENTE DESDE	LO CENTRAL PARA PROVEEDORES	AFECTA A
Reglamento (UE) 2022/2554	17/01/2025	Arts. 28 a 30	Proveedores de TI de entidades financieras de la UE

En pocas palabras

El Reglamento de Resiliencia Operativa Digital, conocido como DORA por su nombre en inglés (Digital Operational Resilience Act), es un reglamento de la UE. Se aplica directamente en todos los Estados miembros, sin ley de transposición. Sus destinatarios son las entidades financieras: bancos, aseguradoras, entidades de pago y de dinero electrónico, empresas de servicios de inversión, gestoras de fondos, proveedores de servicios de criptoactivos y otras. Deben organizar su TI de modo que puedan soportar interrupciones, ataques y caídas.

Gran parte del reglamento trata sobre los proveedores terceros de servicios TIC, es decir, los proveedores externos de servicios de TI. El artículo 28 exige que la entidad financiera evalúe los riesgos de un proveedor antes de contratarlo, registre todos los contratos en un registro de información y tenga una estrategia de salida para los servicios importantes. El artículo 29 trata el riesgo de concentración y menciona expresamente a los proveedores de terceros países: hay que considerar el derecho concursal y la protección de datos del país del proveedor. El artículo 30 establece qué debe figurar en cada contrato.

Para un proveedor de Sudamérica esto significa que su cliente solo puede contratarlo si el contrato tiene ese contenido mínimo y usted entrega la información requerida.

A quién afecta en Sudamérica

Solo tienen obligaciones directas según DORA los proveedores que las autoridades europeas de supervisión, ABE, AESPJ y AEVM (EBA, EIOPA y ESMA por sus siglas en inglés), designan como

proveedores terceros críticos de servicios TIC. La primera lista se publicó el 18/11/2025 con 19 proveedores, sobre todo grandes proveedores de nube, centros de datos, redes y software financiero. Según el artículo 31, apartado 12, un proveedor crítico de un tercer país solo puede ser contratado si constituye una filial en la UE dentro de los doce meses siguientes a su designación.

Lo habitual es verse afectado de forma indirecta. Por ejemplo:

- Fintechs y empresas de software, por ejemplo de São Paulo, Buenos Aires o Bogotá, que desarrollan u operan software de pagos, créditos o seguros para clientes de la UE.
- Equipos nearshore que programan, prueban o mantienen sistemas para bancos europeos.
- Centros de datos y proveedores de hosting con clientes financieros europeos.
- Centros de contacto y proveedores de BPO que trabajan con acceso a sistemas del cliente.
- Proveedores de datos de mercado, de solvencia crediticia o de fraude.

Todos ellos quedan anotados en el registro de información del cliente y deben aceptar las cláusulas contractuales del artículo 30. Según una respuesta de la ABE en su procedimiento de preguntas y respuestas (Q&A 2024_7096), los proveedores intragrupo quedan excluidos de la designación como proveedor crítico. Para las obligaciones contractuales eso no vale.

Un ejemplo: una empresa de software de Montevideo opera para una aseguradora española el portal de siniestros. Antes de renovar el contrato, la aseguradora tiene que revisar dónde están los datos, quién tiene acceso, cuánto tarda el portal en volver a funcionar después de una caída y qué pasa si la empresa de software deja de operar. Las respuestas van a su registro y a su evaluación de riesgos. Si la empresa de software no puede respaldarlas, la aseguradora tiene que cubrir el riesgo de otra forma o cambiar de proveedor.

Plazos

DORA se aplica desde el 17/01/2025. Las entidades financieras tuvieron que adaptar los contratos vigentes y armar sus registros. Quien hoy negocia con un banco de la UE recibe el anexo DORA junto con el contrato marco. Los contratos antiguos sin estas cláusulas se actualizan en la siguiente renovación, a menudo con poco plazo.

FECHA	QUÉ OCURRIÓ
17/01/2025	DORA se aplica en todos los Estados miembros
18/11/2025	Primera lista de proveedores terceros críticos de servicios TIC (19 proveedores)

FECHA	QUÉ OCURRIÓ
12 meses después de la designación	Los proveedores críticos de terceros países necesitan una filial en la UE (art. 31, apartado 12)

La supervisión de los proveedores críticos es estricta. Según el artículo 35, apartado 6, se pueden imponer multas coercitivas de hasta el 1 % del volumen de negocios diario medio a nivel mundial.

Qué piden en concreto los clientes de la UE

El artículo 30 fija qué debe incluir un contrato de servicios TIC. Entre otras cosas: una descripción clara del servicio, los lugares donde se tratan los datos, reglas sobre acceso, inspección y auditoría, derechos de rescisión, el apoyo ante incidentes de seguridad y, en servicios importantes, la participación en las pruebas y ejercicios del cliente. En la práctica, le espera lo siguiente:

- Un anexo contractual DORA que recoja estos puntos. Muchos bancos tienen modelos propios.
- Datos para el registro de información: su código LEI (Legal Entity Identifier), los lugares de tratamiento de datos y los subcontratistas que utiliza.
- Un certificado [ISO/IEC 27001](#) o un [informe SOC 2](#).
- Evidencia de gestión de la continuidad, a menudo según ISO 22301.
- La disposición a recibir en sus instalaciones a los auditores del cliente y del supervisor.
- Un plan de salida que describa cómo el cliente puede recuperar o transferir el servicio de forma ordenada.

El código LEI sorprende a muchos proveedores. Se solicita a través de entidades emisoras autorizadas y hay que renovarlo cada año. Sin él, su cliente no puede registrarlo correctamente.

En funciones esenciales o críticas se suma la participación en pruebas. Las grandes entidades financieras deben realizar con regularidad pruebas de penetración basadas en amenazas, y un proveedor que opera una de esas funciones puede quedar incluido. Defina en el contrato cómo se hace, quién paga y cómo se protege a sus otros clientes.

Sus propios proveedores también entran en la mira. Si trabaja para un banco de la UE sobre una plataforma en la nube o subcontrata partes a profesionales independientes, el cliente quiere saberlo y, en su caso, dar su aprobación.

Primeros pasos

1. Revise cuáles de sus clientes de la UE son entidades financieras. Una empresa de leasing o un proveedor de servicios de pago también puede estar incluido.
2. Solicite un código LEI si todavía no tiene uno.
3. Haga una lista de todos los lugares donde almacena o trata datos de clientes y de todos sus subcontratistas.
4. Lea punto por punto el anexo DORA de su cliente más importante y marque lo que hoy no cumple.
5. Redacte un plan de contingencia y recuperación para los servicios que presta a clientes financieros, y póngalo a prueba.
6. Tenga evidencias, políticas e informes de auditoría disponibles en un solo lugar. Una plataforma GRC como [Sightadel](#) ayuda a mantener todo eso para varios clientes a la vez.

El [diagnóstico UE](#) le da una primera evaluación.

Relación con las certificaciones

DORA no exige ningún certificado obligatorio. Pero los bancos de la UE evalúan a sus proveedores con criterios fijos, y un certificado reconocido acorta mucho esa evaluación. En seguridad de la información ese certificado es [ISO/IEC 27001](#), que en proveedores con clientes en Estados Unidos a menudo se complementa con [SOC 2](#). Quien entrega modelos de IA para decisiones de crédito o detección de fraude debería conocer además el [Reglamento de Inteligencia Artificial](#) e [ISO/IEC 42001](#). Si se tratan datos personales, se aplica siempre también el [RGPD](#). Para proveedores de [Brasil](#), [Argentina](#) y [Uruguay](#), la transferencia de datos es más sencilla gracias a la decisión de adecuación.

DORA y [NIS2](#) se superponen. Para las entidades financieras prevalece DORA como norma especial, pero los requisitos para los proveedores son parecidos. Quien trabaja para ambos grupos de clientes puede atenderlos con un solo sistema de gestión.

FAQ

¿DORA se aplica a mi empresa en Sudamérica?

De forma directa solo si lo designan proveedor tercero crítico de servicios TIC. En los demás casos, las obligaciones le llegan a través del contrato con su cliente financiero de la UE.

¿Qué es un registro de información?

Una lista en la que cada entidad financiera de la UE lleva todos los contratos de servicios TIC, con datos sobre el proveedor, el servicio, la ubicación de los datos y los subcontratistas (art. 28, apartado

3). Usted le entrega esos datos.

¿Tengo que constituir una empresa en la UE?

Solo si lo designan proveedor crítico. En ese caso, el artículo 31, apartado 12, exige una filial en la UE en un plazo de doce meses.

¿Alcanza con un informe SOC 2 para DORA?

Muchos bancos lo aceptan. Pero en Europa está más difundido el certificado ISO/IEC 27001. Encontrará la comparación en [SOC 2 o ISO 27001](#).

¿Qué herramienta ayuda con los requisitos DORA de un cliente?

[Sightadel](#) trae DORA como marco, junto con ISO/IEC 27001, y guarda los datos en Alemania. Allí puede llevar políticas, el plan de contingencia, las evidencias y la lista de subcontratistas. Para las preguntas sobre sistemas accesibles desde internet, un [informe de veyrisk](#) muestra cómo revisa usted su superficie de ataque externa.

Fuentes · Actualizado: 11 de octubre de 2026

Reglamento (UE) 2022/2554 (DORA), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

AEVM (ESMA): designación de proveedores terceros críticos de servicios TIC: <https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers>

ABE (EBA): vigilancia según DORA: <https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/dora-oversight>

ABE (EBA): Q&A 2024_7096: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2024_7096

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel

Sightadel guía a su equipo por DORA: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)

veyrisk

veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>