

PAÍS · MERCOSUR

Brasil: lo que esperan los clientes de la UE

Desde enero de 2026, la UE considera que Brasil ofrece una protección de datos adecuada. Eso facilita los flujos de datos, pero no reemplaza las pruebas de seguridad informática, de no deforestación ni de emisiones.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
LGPD, Lei 13.709/2018	sí, desde 01/2026	UE-Mercosur, provisional desde 01/05/2026	sin ley transversal, PL 4.752/2025 pendiente

Panorama: comercio con la UE

Brasil es el mayor socio comercial de la UE en Sudamérica. Según la Comisión Europea, en 2025 cerca del 42 % de las exportaciones brasileñas a la UE fueron productos agrícolas y el 27 %, combustibles y productos mineros, sobre todo petróleo crudo y, además, mineral de hierro. Por eso, quien envía soja de Paraná, café de Minas Gerais o celulosa de Mato Grosso do Sul a Róterdam o Hamburgo se topa primero con normas de cadena de suministro como el [EUDR](#). A los exportadores de acero y aluminio los alcanza el [CBAM](#).

A eso se suma una exportación creciente de servicios: empresas de software de São Paulo, Florianópolis o Recife desarrollan para bancos, aseguradoras y clientes industriales de Europa. Para ellas, la protección de datos y la seguridad informática pesan más que los aranceles.

Protección de datos: la LGPD frente al RGPD

La LGPD (Lei nº 13.709/2018) rige desde septiembre de 2020, y la ANPD aplica sanciones desde agosto de 2021. Está inspirada en el [RGPD \(Reglamento General de Protección de Datos\)](#): bases legales para cada tratamiento, derechos de los titulares, un encargado de protección de datos (encargado), evaluaciones de impacto y obligaciones de notificación ante incidentes de seguridad. Quien aplica bien la LGPD ya tiene resuelta buena parte de las obligaciones del RGPD.

Desde enero de 2026 existe además una decisión de adecuación de la UE (Decisión de Ejecución (UE) 2026/179). El reconocimiento es mutuo: con la Resolução CD/ANPD nº 32/2026, la ANPD también calificó a la UE como adecuada. Para sus clientes de la UE, esto significa que los datos personales pueden fluir hacia Brasil sin cláusulas contractuales tipo y sin evaluación de impacto de la transferencia. Solo quedan excluidas las transferencias con fines de seguridad pública y persecución penal.

La adecuación regula solo la transferencia de datos. Si trata datos por encargo de un cliente de la UE, sigue necesitando un contrato de encargo del tratamiento según el art. 28 del RGPD y tiene que acreditar sus medidas técnicas y organizativas.

En la práctica se notan dos diferencias. La LGPD contempla diez bases legales, entre ellas la protección del crédito; el RGPD, seis. Y el plazo para notificar violaciones de datos se cuenta en días hábiles, no en horas. Si atiende ambos regímenes, lo mejor es ajustar sus procesos al plazo más corto.

Ciberseguridad frente a NIS2

Brasil todavía no tiene una ley que, como [NIS2](#), fije obligaciones para sectores enteros. El Decreto nº 11.856/2023 establece la política nacional de ciberseguridad (PNCiber) y un comité (CNCiber), pero no crea una autoridad de supervisión con potestades sobre las empresas. El proyecto de Marco Legal da Cibersegurança (PL 4.752/2025) está en el Senado. Lo que sigue abierto, sobre todo, es si la supervisión quedará a cargo de una nueva agencia o de la Anatel.

Por ahora, las exigencias vinculantes son sectoriales. Según la Resolução CMN nº 4.893/2021, los bancos tienen que contar con una política de ciberseguridad, gestionar la tercerización en la nube y notificar los incidentes relevantes al Banco Central. Para las instituciones de pago rige algo equivalente según la Resolução BCB nº 85/2021.

Para los proveedores de clientes europeos, esto es secundario. Su cliente en la UE tiene que gestionar la seguridad de su cadena de suministro según NIS2 y le traslada esa obligación por contrato. Quien provee software a entidades financieras de la UE recibe además cláusulas de [DORA](#) en el contrato, y los fabricantes de productos conectados quedan alcanzados por el [Reglamento de Ciberresiliencia \(CRA\)](#).

Plazos de notificación comparados

MOTIVO	BRASIL	UE
Violación de datos ante la autoridad	3 días hábiles desde que se tiene conocimiento, si hay riesgo relevante (Res. CD/ANPD 15/2024); plazo doble para pequeñas empresas	72 horas (art. 33 RGPD)
Información a los afectados	también 3 días hábiles	sin dilación indebida si hay alto riesgo (art. 34 RGPD)

MOTIVO	BRASIL	UE
Ciberincidente significativo	sin ley general; los bancos notifican al Banco Central	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

La norma de la ANPD exige además que documente los incidentes y conserve esos registros durante cinco años. Un cliente de la UE suele fijar en su contrato un plazo propio, a menudo de 24 a 48 horas, para poder cumplir sus 72 horas.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	ANPD, Autoridade Nacional de Proteção de Dados
Ciberseguridad federal	GSI/PR con CTIR Gov (administración federal)
CSIRT del sector privado	CERT.br del NIC.br
Sector financiero	Banco Central do Brasil, Conselho Monetário Nacional
Acreditación	INMETRO, acreditación a cargo de la Cgcre

Los certificados de organismos acreditados por la Cgcre suelen reconocerse en la UE, porque la Cgcre forma parte de los acuerdos internacionales de reconocimiento entre organismos de acreditación. Aun así, pregunte antes de la auditoría si su cliente exige un certificador en particular.

Lo que suelen exigir los clientes de la UE

Para los exportadores agrícolas y de materias primas, el EUDR está en primer plano. Su comprador necesita los geodatos de sus parcelas y la prueba de que allí no hubo deforestación después del 31/12/2020. En el EUDR, Brasil está clasificado como país de riesgo estándar. Por eso rige la diligencia debida completa; la diligencia debida simplificada del art. 13 solo existe para países de riesgo bajo. En la cadena alimentaria se suman certificados [IFS](#), [BRCGS](#) o [FSSC 22000](#).

Los proveedores de software y TI suelen recibir un cuestionario de seguridad basado en NIS2 e [ISO 27001](#). Preguntas típicas: ¿con qué rapidez notifica un incidente? ¿Quién tiene acceso a los datos de producción? ¿Se hacen pruebas de penetración? Un certificado ISO 27001 responde muchas de estas preguntas de una vez. El sistema de gestión se puede armar y preparar para la auditoría en una plataforma GRC como [Sightadel](#); el certificado lo emite después un organismo acreditado.

Muchos clientes también revisan desde afuera lo que usted expone en internet: puertos abiertos, certificados vencidos, versiones viejas de servidores. Quien lo monitorea de forma continua, por ejemplo con [veyrisk](#), conoce la respuesta antes de que llegue el cuestionario.

En el contrato, estos requisitos suelen figurar como anexo: un contrato de encargo del tratamiento según el art. 28 del RGPD, una lista de medidas técnicas y organizativas, plazos de notificación de incidentes, derechos de auditoría del cliente y reglas para subencargados. Como Brasil se considera adecuado, no hacen falta las cláusulas contractuales tipo. El resto su cliente lo exige igual, y lo va a volver a revisar en la renovación.

Un punto de partida razonable para empresas brasileñas:

1. Verifique qué normas de la UE afectan a sus clientes y pregunte activamente por los requisitos, en lugar de esperar el cuestionario.
2. Compare su documentación de la LGPD con los requisitos del RGPD. El registro de actividades de tratamiento, las bases legales y las evaluaciones de impacto suelen poder reutilizarse.
3. Implemente un proceso de notificación que cumpla el plazo contractual más corto y practíquelo una vez al año.
4. Para el EUDR, reúna los geodatos y las pruebas de sus proveedores antes de que el comprador los pida.
5. Decida si un certificado ISO 27001 o una norma alimentaria responde los cuestionarios de sus clientes más rápido que cualquier respuesta individual.

En qué punto está hoy se lo muestra el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

El [Acuerdo UE-Mercosur](#) se firmó el 17/01/2026 en Asunción. Su parte comercial, el Acuerdo Comercial Interino, se aplica de forma provisional desde el 01/05/2026 entre la UE y Brasil, Argentina, Paraguay y Uruguay. Los aranceles bajan de forma escalonada, y para aprovechar la preferencia necesita una declaración de origen. El Acuerdo de Asociación completo sigue en proceso de ratificación.

En la práctica, esto significa: verifique para cada producto el arancel, el calendario de desgravación y la regla de origen. Todo eso está en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en el Mercosur. Para algunos productos agrícolas rigen cupos arancelarios, es decir, cantidades limitadas con arancel preferencial. Su importador en la UE suele conocer estas reglas mejor que usted y puede ayudarle a incluir correctamente la declaración de origen en la factura. Conserve las pruebas de origen durante varios años, porque la aduana puede hacer controles

posteriores.

El acuerdo no exime del derecho de la UE. El EUDR, el CBAM, el RGPD y las normas de producto se aplican a las mercaderías brasileñas igual que a las de cualquier otro país.

FAQ

¿Siguen necesitando los clientes de la UE cláusulas contractuales tipo para transferir datos a Brasil?

No. Desde la decisión de adecuación (UE) 2026/179 de enero de 2026, los datos pueden transferirse a Brasil sin cláusulas contractuales tipo. Si usted trata datos por encargo, sigue siendo necesario un contrato de encargo del tratamiento.

¿Existe en Brasil una ley como NIS2?

Todavía no. El proyecto PL 4.752/2025 está en el Senado. Mientras tanto rigen normas sectoriales, sobre todo para bancos e instituciones de pago.

¿En cuánto tiempo tengo que notificar una violación de datos a la ANPD?

Dentro de los tres días hábiles desde que se tiene conocimiento, si existe un riesgo relevante para los titulares (Resolução CD/ANPD 15/2024). Las pequeñas empresas tienen el doble de plazo.

¿El Acuerdo UE-Mercosur reduce mis obligaciones bajo el EUDR?

No. Las ventajas arancelarias solo se obtienen con prueba de origen, y el EUDR rige sin cambios. Más información en la página sobre el [EUDR](#).

¿Qué ayuda a responder el cuestionario de seguridad de un cliente de la UE?

Tener políticas, riesgos y evidencias ya documentados. En [Sightadel](#) se arma un sistema de gestión según ISO 27001 o NIS2, y lo elaborado para un marco se aprovecha para el siguiente. Para las preguntas sobre su exposición en internet, el [informe de veyrisk](#) muestra servicios abiertos, certificados y vulnerabilidades vistos desde afuera.

Fuentes · Actualizado: 11 de octubre de 2026

Lei nº 13.709/2018 (LGPD), Planalto: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ANPD, Autoridade Nacional de Proteção de Dados: <https://www.gov.br/anpd>

Comisión Europea: decisiones de adecuación: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Decreto nº 11.856/2023 (PNCiber), Planalto: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm

CERT.br: <https://cert.br/>

Comisión Europea, DG Comercio: Brasil: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/brazil_en

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

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por NIS2: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)



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 →](#)



Valar es un firewall de hardware con software de neonotu. Protege oficinas y sedes y genera los registros que exigen NIS2 e ISO 27001.

[Ver Valar →](#)

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>