

INFORME POR PAÍS

Sudamérica y la UE: comparación legal

Protección de datos, ciberseguridad, plazos de notificación, autoridades y acuerdos comerciales de Argentina, Brasil, Paraguay, Uruguay, Bolivia, Chile, Colombia, Perú y Ecuador.

16 DE OCTUBRE DE 2026 · [HTTPS://WWW.MERCOEU.COM](https://www.mercoeu.com)

Contenido

1. Su país frente al derecho de la UE
2. Argentina: lo que esperan los clientes de la UE
3. Brasil: lo que esperan los clientes de la UE
4. Paraguay: lo que esperan los clientes de la UE
5. Uruguay: lo que esperan los clientes de la UE
6. Bolivia: lo que esperan los clientes de la UE
7. Chile: lo que esperan los clientes de la UE
8. Colombia: lo que esperan los clientes de la UE
9. Perú: lo que esperan los clientes de la UE
10. Ecuador: lo que esperan los clientes de la UE

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

PAÍSES · RESUMEN

Su país frente al derecho de la UE

Para cada uno de los nueve países mostramos en qué punto está la legislación local, en qué se diferencia del RGPD y de NIS2 y qué acuerdo rige con la UE.

Los nueve países de un vistazo

PAÍS	LEY DE PROTECCIÓN DE DATOS	LEY DE CIBERSEGURIDAD	ADECUACIÓN DE LA UE	ACUERDO COMERCIAL CON LA UE
Argentina	Ley 25.326 (2000), reforma en el Congreso	ninguna	sí (2003)	UE-Mercosur, provisional desde 01/05/2026
Brasil	LGPD, Lei 13.709/2018	ninguna, proyecto PL 4.752/2025	sí (desde 01/2026)	UE-Mercosur, provisional desde 01/05/2026
Paraguay	Ley 7593/2025, plena desde fines de 11/2027	ninguna	no	UE-Mercosur, provisional desde 01/05/2026
Uruguay	Ley 18.331 (2008), Ley 19.670	Ley 20.212 art. 78 y ss., Decreto 66/025	sí (2012)	UE-Mercosur, provisional desde 01/05/2026
Bolivia	ninguna	ninguna	no	ninguno; preferencias arancelarias vía SPG+
Chile	Ley 21.719, vigente desde 01/12/2026 (aplazamiento solicitado)	Ley 21.663 (2024)	no	Acuerdo Comercial Interino desde 01/02/2025
Colombia	Ley 1581 de 2012	ninguna, Decreto 338/2022	no	Acuerdo Comercial desde 2013
Perú	Ley 29733, DS 016-2024-JUS	marco mediante DU 007-2020 y DS 126-2025-PCM	no	Acuerdo Comercial desde 2013

PAÍS	LEY DE PROTECCIÓN DE DATOS	LEY DE CIBERSEGURIDAD	ADECUACIÓN DE LA UE	ACUERDO COMERCIAL CON LA UE
Ecuador	LOPDP (2021)	Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026)	no	Acuerdo Comercial desde 2017

Qué cambia para usted con la adecuación

Para Argentina, Uruguay y, desde enero de 2026, también Brasil, la UE determinó que la protección de datos es equivalente. Sus clientes de la UE pueden transferir datos a esos países sin firmar cláusulas contractuales tipo. Para los otros seis países necesitan esas cláusulas y una evaluación de impacto de la transferencia. El contrato de encargado del tratamiento según el [RGPD \(Reglamento General de Protección de Datos\)](#) lo necesita en los nueve países.

Ciberseguridad: pocas leyes, muchos contratos

El país más cercano a [NIS2](#) es Chile, donde la alerta temprana vence a las tres horas. Uruguay exige a los sectores críticos una notificación dentro de las 24 horas. Ecuador tiene una ley propia desde mayo de 2026 y Perú regula las notificaciones de los servicios digitales por vía reglamentaria. En los demás países rigen sobre todo las exigencias de la supervisión bancaria.

De todos modos, para un proveedor la legislación local es solo una parte. Los clientes de la UE trasladan por contrato sus obligaciones derivadas de NIS2, [DORA](#) y el [Reglamento de Ciberresiliencia \(CRA\)](#), sin importar en qué país esté su empresa. Para responder esos requisitos con evidencias sirve una plataforma GRC como [Sightadel](#), que cubre NIS2, DORA e ISO 27001, entre otros marcos.

Acuerdos y cadena de suministro

El [Acuerdo UE-Mercosur](#) se aplica de forma provisional desde el 01/05/2026 con Argentina, Brasil, Paraguay y Uruguay. Bolivia es miembro del Mercosur, pero no participa. Chile, Colombia, Perú y Ecuador tienen acuerdos propios. Ninguno de ellos exime del [EUDR](#) ni del [CBAM](#).

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

<https://www.mercoeu.com/es/paises>

PAÍS · MERCOSUR

Argentina: lo que esperan los clientes de la UE

Desde 2003, la UE considera que Argentina ofrece una protección de datos adecuada. La ley que lo sustenta es del año 2000 y hay una reforma en el Congreso. No existe una ley de ciberseguridad.

Panorama: comercio con la UE

Según la Comisión Europea, cerca de dos tercios de las exportaciones argentinas a la UE en 2025 fueron productos agrícolas, sobre todo oleaginosas y proteaginosas como la soja y los alimentos para animales que se obtienen de ella. Los productos químicos representaron el 13,7 % y los combustibles y productos mineros, el 6,7 %. Por eso, quien vende harina de soja de Rosario o carne vacuna de la Pampa a Europa tiene que ocuparse sobre todo del [EUDR](#).

Además, Argentina tiene un sector de software fuerte. Equipos de desarrollo de Buenos Aires, Córdoba y Mendoza trabajan desde hace años para clientes de España, Alemania y los Países Bajos. Para ellos, lo central son la protección de datos y la seguridad informática.

Protección de datos: la Ley 25.326 frente al RGPD

La base es la Ley 25.326 de Protección de los Datos Personales, del año 2000, con su reglamentación, el Decreto 1558/2001. La autoridad competente es la AAIP (Agencia de Acceso a la Información Pública). La ley contempla el consentimiento, la finalidad, los derechos de acceso y supresión y un registro de bases de datos. Falta mucho de lo que el [RGPD \(Reglamento General de Protección de Datos\)](#) desarrolló después: evaluaciones de impacto, un delegado de protección de datos obligatorio, multas calculadas como porcentaje de la facturación y un plazo legal para notificar violaciones de seguridad.

Aun así, en 2003 la UE reconoció a Argentina como país adecuado (Decisión 2003/490/CE) y lo confirmó en el informe de la Comisión del 15/01/2024. Argentina ratificó además el Convenio 108+ modernizado del Consejo de Europa. Sus clientes de la UE pueden, por lo tanto, transferir datos personales a Argentina sin cláusulas contractuales tipo.

Reforma en el Congreso: el proyecto 3397-D-2026 se presentó el 16/07/2026 en la Cámara de Diputados. Prevé, entre otras cosas, un plazo para notificar violaciones de seguridad y multas

más altas. Hasta que se apruebe, la Ley 25.326 sigue vigente sin cambios.

Si ya trabaja con el estándar del RGPD, tendrá poco que ajustar cuando llegue la reforma. Para proveedores con clientes en la UE es de todos modos el camino razonable, porque el contrato de encargo del tratamiento según el art. 28 del RGPD exige esos estándares con independencia del derecho argentino.

Ciberseguridad frente a NIS2

Argentina no tiene una ley de ciberseguridad. Hay una estrategia nacional de ciberseguridad y un equipo estatal de respuesta, CERT.ar, en la Dirección Nacional de Ciberseguridad. De ahí no surgen obligaciones para las empresas como las que [NIS2](#) prevé en la UE para energía, transporte, salud o servicios digitales.

Hay exigencias vinculantes en el sector financiero. El BCRA establece, con la Comunicación «A» 7724, estándares mínimos de tecnología y seguridad de la información, y regula en otras comunicaciones la respuesta ante ciberincidentes y su notificación. Si provee software o servicios de centro de datos a bancos argentinos, conoce estos requisitos por los contratos.

Para los clientes de la UE, al final cuenta lo que dice el contrato. Una empresa de software de Córdoba que desarrolla para una aseguradora alemana recibe cláusulas derivadas de [DORA](#). Un fabricante de controladores con conexión de red tiene que cumplir el [Reglamento de Ciberresiliencia \(CRA\)](#) si el equipo se vende en la UE.

Plazos de notificación comparados

MOTIVO	ARGENTINA	UE
Violación de datos ante la autoridad	sin plazo legal en la Ley 25.326	72 horas (art. 33 RGPD)
Información a los afectados	sin plazo legal	sin dilación indebida si hay alto riesgo (art. 34 RGPD)
Ciberincidente significativo	sin ley general; los bancos notifican según las normas del BCRA	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Como la ley local no fija un plazo, en la práctica lo fija su cliente de la UE en el contrato. Cuente con 24 a 48 horas y organice su proceso para poder cumplirlo: quién decide, quién notifica y qué datos van en la primera notificación.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	AAIP, Dirección Nacional de Protección de Datos Personales
CSIRT	CERT.ar, Dirección Nacional de Ciberseguridad
Sector financiero	BCRA, Banco Central de la República Argentina
Acreditación	OAA, Organismo Argentino de Acreditación

Los certificados [ISO 27001](#) o [ISO 9001](#) emitidos por organismos acreditados por el OAA se reconocen por lo general en la UE. Algunos grupos insisten en un certificador que conocen. Aclárelo antes de la auditoría.

Lo que suelen exigir los clientes de la UE

Los exportadores agrícolas necesitan, para el EUDR, los geodatos de todas las parcelas donde se produjo la soja o el ganado de la mercadería destinada a la UE, y la prueba de que allí no hubo deforestación desde el 31/12/2020. Argentina está clasificada como país de riesgo estándar. A los fabricantes de alimentos se les pide además [IFS](#), [BRCGS](#) o [FSSC 22000](#).

Los proveedores de TI reciben cuestionarios de seguridad, un contrato de encargo del tratamiento y, a menudo, el pedido de un certificado ISO 27001 o un informe SOC 2. Un sistema de gestión de seguridad de la información se puede armar y documentar para la auditoría con una plataforma GRC como [Sightadel](#), que se desarrolla y se aloja en Alemania. Para las preguntas sobre lo que su empresa expone en internet, [veyrisk](#) revisa desde afuera servicios abiertos, certificados y la configuración de DNS y correo, y entrega un informe que puede adjuntar a la respuesta.

En la práctica, los proveedores argentinos reciben un paquete de varios documentos: el contrato de encargo del tratamiento, un anexo con medidas técnicas y organizativas, una lista de subencargados, un acuerdo de confidencialidad y un cuestionario de seguridad que muchas veces supera las cien preguntas. Las cláusulas contractuales tipo no hacen falta gracias a la adecuación. Pero si usted transfiere datos a proveedores fuera de Argentina, por ejemplo a un proveedor cloud en EE. UU., su cliente de la UE le va a preguntar cómo está protegida esa transferencia.

Un punto de partida razonable para empresas argentinas:

1. Aclare cuáles de sus clientes están en la UE y qué normas de la UE se les aplican.
2. Lleve su esquema de protección de datos al nivel del RGPD, también donde la Ley 25.326 exige menos. Eso lo prepara al mismo tiempo para la reforma.

3. Fije un plazo interno de notificación de incidentes más corto que cualquier plazo de sus contratos.
4. Para las exportaciones agrícolas, reúna los geodatos de sus parcelas y los de sus proveedores.
5. Evalúe si un certificado ISO 27001 o una norma alimentaria le ahorra pruebas individuales.

Un primer panorama de sus brechas se lo da el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

El [Acuerdo UE-Mercosur](#) se firmó el 17/01/2026 en Asunción. Argentina lo ratificó en febrero de 2026. Desde el 01/05/2026 se aplica de forma provisional la parte comercial entre la UE y Argentina, Brasil, Paraguay y Uruguay. Para la preferencia arancelaria 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.

Las ventajas arancelarias no cambian el derecho de producto de la UE. El EUDR, el CBAM y el RGPD siguen rigiendo por completo.

<https://www.mercoeu.com/es/paises/argentina>

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA

**Sightadel**

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.

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.

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 (encarregado), 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)
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.

<https://www.mercoeu.com/es/paises/brasil>

PAÍS · MERCOSUR

Paraguay: lo que esperan los clientes de la UE

Desde noviembre de 2025, Paraguay tiene una ley general de protección de datos que, tras un período de transición, será plenamente aplicable a fines de noviembre de 2027. Todavía no hay una ley de ciberseguridad.

Panorama: comercio con la UE

Las importaciones de la UE desde Paraguay son casi en su totalidad productos agrícolas: según la Comisión Europea, en 2025 representaron el 82 %. La soja del este del país y la carne vacuna del Chaco son los ejemplos más conocidos. Las dos quedan alcanzadas por el [EUDR](#), y es justamente ahí donde empiezan las preguntas de los compradores europeos.

Para Paraguay, el Acuerdo UE-Mercosur es el paso de política comercial más importante en años. Asunción fue la sede de la firma, el 17/01/2026.

Protección de datos: la Ley 7593/2025 frente al RGPD

Hasta 2025, Paraguay no tenía una ley general de protección de datos; estaban regulados sobre todo los datos crediticios (Ley 6534/2020). La Ley N° 7593/2025 de Protección de Datos Personales se promulgó el 27/11/2025. Prevé un período de transición de 24 meses, por lo que será plenamente aplicable desde fines de noviembre de 2027. La reglamentación todavía está pendiente.

La ley retoma muchas ideas básicas del [RGPD \(Reglamento General de Protección de Datos\)](#): bases legales, derechos de los titulares, obligaciones para responsables y encargados, reglas para las transferencias internacionales. La autoridad de control será una Agencia Nacional de Protección de Datos Personales, ubicada en el Ministerio de Tecnologías de la Información y Comunicación (MITIC) con autonomía funcional. Las multas van de 20 a 10.000 jornales mínimos.

Paraguay no tiene una decisión de adecuación de la UE. Sus clientes de la UE necesitan, para cada transferencia de datos personales a Paraguay, cláusulas contractuales tipo (Decisión de Ejecución (UE) 2021/914) y una evaluación de impacto de la transferencia. Esto vale también para casos sencillos, por ejemplo cuando su equipo comercial en Asunción consulta datos de clientes en el CRM de un distribuidor alemán.

No necesita esperar hasta 2027. Si ahora arma un registro de actividades de tratamiento, ordena los accesos y define un proceso de notificación de violaciones de datos, cumple con lo que esperan los clientes de la UE y queda preparado para la nueva ley.

Ciberseguridad frente a NIS2

Paraguay no tiene una ley de ciberseguridad. Hay varios proyectos en el Congreso, entre ellos una «Ley de Ciberseguridad de la República del Paraguay», presentada en junio de 2025. Por ahora, la base es la Estrategia Nacional de Ciberseguridad 2025 a 2028 (Decreto N° 3900/2025). El equipo nacional de respuesta, CERT-PY, depende de la Dirección General de Ciberseguridad del MITIC.

De ahí no se derivan para las empresas obligaciones como las de [NIS2](#), es decir, gestión de riesgos, seguridad de la cadena de suministro y plazos fijos de notificación para sectores enteros. Para los bancos, el Banco Central tiene sus propias exigencias de seguridad de la información.

Para los proveedores paraguayos esto significa que los requisitos llegan a través del contrato con el cliente de la UE. A un comerciante agrícola con software de logística propio le preguntarán por control de acceso, copias de seguridad y planes de contingencia; a un fabricante de equipos conectados, por el [Reglamento de Ciberresiliencia \(CRA\)](#).

Plazos de notificación comparados

MOTIVO	PARAGUAY	UE
Violación de datos ante la autoridad	hoy sin plazo vigente; Ley 7593/2025 desde fines de 11/2027, detalles por reglamentación	72 horas (art. 33 RGPD)
Información a los afectados	hoy sin plazo vigente	sin dilación indebida si hay alto riesgo (art. 34 RGPD)
Ciberincidente significativo	sin ley	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

En la práctica, el cliente de la UE fija el plazo en el contrato, por lo general de 24 a 48 horas. Defina de antemano quién notifica en su empresa y quién está disponible si el incidente ocurre un fin de semana.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	Agencia Nacional de Protección de Datos Personales (MITIC, en formación)
Ciberseguridad, CSIRT	MITIC, Dirección General de Ciberseguridad con CERT-PY
Sector financiero	BCP, Banco Central del Paraguay
Acreditación	ONA, Organismo Nacional de Acreditación (del CONACYT)

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del ONA o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

Para los exportadores de soja y carne, el EUDR está en primer lugar: geodatos de todas las parcelas, prueba de origen libre de deforestación después del 31/12/2020 y prueba de producción legal según el derecho paraguayo. En el EUDR, Paraguay está clasificado como país de riesgo estándar. Justamente en el Chaco, donde en las últimas décadas se taló mucho bosque, los compradores preguntan con detalle.

Los fabricantes de alimentos suelen necesitar un certificado [IFS](#), [BRCGS](#) o [FSSC 22000](#); las plantas industriales, a menudo [ISO 9001](#). Quien trata datos de clientes europeos recibe cláusulas contractuales tipo y un cuestionario de seguridad. El registro de actividades de tratamiento, las medidas técnicas y organizativas y las respuestas a esos cuestionarios se pueden llevar juntos en una plataforma como [Sightadel](#), que se aloja en Alemania.

En el contrato, estos requisitos suelen figurar en varios anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Su cliente de la UE tiene que elaborar además una evaluación de impacto de la transferencia para Paraguay. Para eso necesita que usted le informe sobre accesos, cifrado y posibles requerimientos de autoridades. Cuanto más precisas sean sus respuestas, antes se firma el contrato. Si le preguntan también qué sistemas tiene accesibles desde internet, un análisis externo como el de [veyrisk](#) le da esa respuesta por escrito.

Un punto de partida razonable para empresas paraguayas:

1. Aclare qué datos recibe de clientes de la UE y dónde se almacenan.
2. Arme un registro de actividades de tratamiento y designe a una persona responsable de la protección de datos. Ambas cosas las va a necesitar a más tardar con la Ley 7593/2025.
3. Implemente un proceso de notificación de incidentes que cumpla los plazos de sus contratos.
4. Para las exportaciones de soja y carne, reúna los geodatos de sus parcelas y los de sus proveedores.
5. Verifique qué certificado piden sus clientes con más frecuencia y planifique la auditoría a tiempo.

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

Acuerdo con la UE

El [Acuerdo UE-Mercosur](#) se firmó el 17/01/2026 en Asunción. Desde el 01/05/2026 se aplica de forma provisional la parte comercial entre la UE y Paraguay, Argentina, Brasil y Uruguay. Para la preferencia arancelaria 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 ayudarlo 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 baja los aranceles, no los requisitos. El EUDR, el CBAM y el RGPD se aplican por completo a las mercaderías paraguayas.

<https://www.mercoeu.com/es/paises/paraguay>

PAÍS · MERCOSUR

Uruguay: lo que esperan los clientes de la UE

Uruguay tiene el derecho de protección de datos más desarrollado del Mercosur y una decisión de adecuación de la UE desde 2012. Para los sectores críticos rige la obligación de notificar ciberincidentes dentro de las 24 horas.

Panorama: comercio con la UE

Según la Comisión Europea, más de la mitad de las importaciones de la UE desde Uruguay en 2025 fueron celulosa y papel (52 %). Les siguen los productos de origen animal (21 %), sobre todo carne vacuna, y los productos vegetales (11 %). Las plantas de celulosa sobre el río Uruguay y los frigoríficos del interior quedan así directamente alcanzados por el [EUDR](#), que abarca la madera y el ganado vacuno.

Al mismo tiempo, Montevideo es uno de los polos de software más importantes de América Latina. Muchas empresas desarrollan allí para clientes de España, Alemania o Escandinavia y, en ese trabajo, tratan datos personales provenientes de la UE.

Protección de datos: la Ley 18.331 frente al RGPD

La Ley 18.331 de Protección de Datos Personales es de 2008 y su reglamentación es el Decreto 414/009. Con la Ley 19.670 de 2018 y el Decreto 64/020, Uruguay acercó su normativa al [RGPD](#) ([Reglamento General de Protección de Datos](#)): la ley se aplica también a responsables en el exterior cuando tratan datos de personas en Uruguay, existe la obligación de notificar violaciones de seguridad y ciertas entidades deben designar un delegado de protección de datos. La autoridad de control es la URCDP (Unidad Reguladora y de Control de Datos Personales), en la órbita de AGESIC.

En 2012, la UE reconoció a Uruguay como país adecuado mediante la Decisión de Ejecución 2012/484/UE y lo confirmó en el informe de la Comisión del 15/01/2024. Uruguay ratificó además el Convenio 108+ del Consejo de Europa. Sus clientes de la UE pueden, por lo tanto, transferir datos a Uruguay sin cláusulas contractuales tipo.

Para los encargados del tratamiento, la adecuación cambia poco en el papeleo: el contrato según el art. 28 del RGPD, la lista de subencargados y la acreditación de las medidas técnicas y organizativas siguen siendo obligatorios.

Ciberseguridad frente a NIS2

Uruguay es uno de los pocos países de la región con obligaciones legales de ciberseguridad fuera del sector financiero. La Ley 20.212 (Rendición de Cuentas 2022) obliga, en su art. 78 y siguientes, a los organismos públicos y a los operadores privados de sectores críticos a notificar los incidentes de seguridad dentro de las 24 horas. El Decreto 66/025 regula la aplicación: notificación al CERTuy, designación de responsables de seguridad, conservación de registros y aplicación del Marco de Ciberseguridad, un marco nacional con controles similares a los de ISO 27001.

Comparado con [NIS2](#), el universo de obligados es menor. En la UE, NIS2 abarca también a medianas empresas de 18 sectores, entre ellos la fabricación de alimentos y los servicios digitales. En Uruguay, la obligación recae en los sectores críticos. Con 24 horas, sin embargo, la primera notificación es tan rápida como la alerta temprana de NIS2.

Para los proveedores de clientes europeos se suman los requisitos contractuales: cláusulas de NIS2 sobre la cadena de suministro, [DORA](#) si el cliente es del sector financiero y el [Reglamento de Ciberresiliencia \(CRA\)](#) para productos con elementos digitales.

Plazos de notificación comparados

MOTIVO	URUGUAY	UE
Violación de datos ante la autoridad	72 horas desde que se tiene conocimiento, ante la URCDP (Decreto 64/020, art. 4)	72 horas (art. 33 RGPD)
Primeras medidas tras una violación de datos	iniciarlas dentro de las 24 horas (Decreto 64/020, art. 3)	sin plazo propio
Ciberincidente, sectores críticos	24 horas ante el CERTuy (Ley 20.212, Decreto 66/025)	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Los plazos para violaciones de datos son iguales en Uruguay y en la UE. Por eso resulta sencillo armar un proceso que sirva para ambos.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	URCDP, en la órbita de AGESIC

ÁREA	ORGANISMO
Ciberseguridad, CSIRT	AGESIC con CERTuy
Sector financiero	BCU, Banco Central del Uruguay
Acreditación	OUA, Organismo Uruguayo de Acreditación

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del OUA o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

Una empresa de software de Montevideo que desarrolla para un banco de Madrid recibe un cuestionario de seguridad, un contrato según el art. 28 del RGPD y cláusulas de DORA sobre derechos de auditoría y planes de salida. A menudo se espera un certificado [ISO 27001](#). Quien ya trabaja con el Marco de Ciberseguridad tiene implementada buena parte de los controles. El resto se puede completar y preparar para la auditoría en una plataforma GRC como [Sightadel](#).

Muchos clientes de la UE revisan además la superficie de ataque visible desde afuera de sus proveedores. Con [veyrisk](#) usted ve esos mismos hallazgos y puede corregirlos antes de que pregunte el cliente.

Los exportadores de celulosa y madera necesitan, para el EUDR, los geodatos de las plantaciones y la prueba de origen libre de deforestación. Los exportadores de carne necesitan los mismos datos para las superficies de pastoreo y, además, certificados alimentarios [IFS](#), [BRCGS](#) o [FSSC 22000](#).

En el contrato, estos requisitos suelen aparecer como anexos: contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación, derechos de auditoría y una lista de subencargados. Por la adecuación, no hacen falta las cláusulas contractuales tipo. Si usted mismo usa proveedores en países sin adecuación, por ejemplo un equipo de soporte en Asia, su cliente de la UE querrá saber cómo está protegida esa transferencia.

Un punto de partida razonable para empresas uruguayas:

1. Verifique si pertenece a un sector crítico según la Ley 20.212. En ese caso, la notificación en 24 horas al CERTuy ya rige para usted.

2. Compare su documentación según la Ley 18.331 y la Ley 19.670 con los requisitos del RGPD. Las brechas suelen ser pequeñas.
3. Arme un proceso de notificación común para la URCDP, el CERTuy y sus clientes de la UE.
4. Revise hasta qué punto sus controles según el Marco de Ciberseguridad ya cubren los requisitos de ISO 27001.
5. Para las exportaciones de madera, celulosa y carne, reúna los geodatos para el EUDR.

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

Acuerdo con la UE

El [Acuerdo UE-Mercosur](#) se firmó el 17/01/2026 en Asunción y Uruguay lo ratificó en febrero de 2026. Desde el 01/05/2026 se aplica de forma provisional la parte comercial entre la UE y Uruguay, Argentina, Brasil y Paraguay. La preferencia arancelaria requiere 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 ayudarlo 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.

Pese al acuerdo, el derecho de la UE se aplica por completo, incluidos el EUDR, el CBAM y el RGPD.

<https://www.mercoeu.com/es/paises/uruguay>

PAÍS · MERCOSUR

Bolivia: lo que esperan los clientes de la UE

Bolivia es miembro pleno del Mercosur desde 2024, pero todavía está incorporando sus normas de forma gradual. No hay una ley de protección de datos ni una ley de ciberseguridad. Los clientes de la UE cubren ese vacío con contratos.

Panorama: comercio con la UE

Bolivia exporta a Europa sobre todo materias primas y productos agrícolas, por ejemplo minerales del Altiplano, castaña amazónica de la zona de Riberalta y quinua. La Comisión no publica un desglose solo para Bolivia. Para el conjunto de los países andinos, menciona como grupos principales en 2025 los productos agrícolas, los productos minerales y la pesca.

Bolivia no tiene un acuerdo comercial con la UE. Las ventajas arancelarias llegan a través del Sistema de Preferencias Generalizadas de la UE, incluido el régimen especial SPG+ de estímulo del desarrollo sostenible y la buena gobernanza. Estas preferencias están sujetas al cumplimiento de convenios internacionales sobre derechos humanos, trabajo y medio ambiente.

Protección de datos frente al RGPD

Bolivia no tiene una ley general de protección de datos. La privacidad está protegida por la Constitución, que prevé una acción específica para su defensa (Acción de Protección de Privacidad, comparable al hábeas data de otros países), y por el derecho procesal constitucional. Se discutieron proyectos de ley de protección de datos, pero ninguno fue promulgado. Por eso no hay autoridad de protección de datos ni obligación legal de notificar violaciones de datos.

El [RGPD \(Reglamento General de Protección de Datos\)](#) es independiente de eso. Se le aplica directamente si usted ofrece bienes o servicios dirigidos a personas en la UE. Y se le aplica por contrato si trata datos por encargo de un cliente de la UE.

No existe una decisión de adecuación de la UE. Para cada transferencia de datos personales a Bolivia, su cliente de la UE necesita cláusulas contractuales tipo (Decisión de Ejecución (UE) 2021/914) y una evaluación de impacto de la transferencia. En esa evaluación analiza si el derecho boliviano socava la protección de los datos. Como falta una ley de protección de datos, le va a exigir medidas técnicas adicionales, por ejemplo cifrado y reglas de acceso estrictas.

Sin una ley local como referencia, sus propias reglas son la prueba. Un esquema de protección de datos por escrito, un registro de actividades de tratamiento y un proceso de notificación ya practicado pesan más en la evaluación de impacto de la transferencia que cualquier promesa.

Ciberseguridad frente a NIS2

Bolivia no tiene una ley de ciberseguridad. Las exigencias de seguridad de la información rigen sobre todo para la administración pública. El equipo de respuesta CGII (Centro de Gestión de Incidentes Informáticos) depende de la agencia estatal de gobierno electrónico y TIC, la AGETIC. En el sector financiero, el supervisor ASFI tiene sus propios requisitos de seguridad de la información.

Esto no es comparable con [NIS2](#). En la UE, NIS2 obliga a medianas y grandes empresas de 18 sectores a la gestión de riesgos, la seguridad de la cadena de suministro y plazos fijos de notificación. Sus clientes de la UE tienen que cumplir esas obligaciones y las trasladan por contrato a sus proveedores, es decir, también a usted.

Si vende en la UE equipos con software o conexión de red, queda además alcanzado por el [Reglamento de Ciberresiliencia \(CRA\)](#).

Plazos de notificación comparados

MOTIVO	BOLIVIA	UE
Violación de datos ante la autoridad	sin obligación, sin autoridad	72 horas (art. 33 RGPD)
Información a los afectados	sin obligación	sin dilación indebida si hay alto riesgo (art. 34 RGPD)
Ciberincidente significativo	sin ley; exigencias para la administración y el sector financiero	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Como la ley local no establece nada, rige el plazo de su contrato. Los clientes de la UE suelen exigir una notificación dentro de las 24 a 48 horas. Defina quién notifica y qué datos incluye la primera notificación.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO

Protección de datos	sin autoridad
Ciberseguridad, CSIRT	AGETIC con CGII
Sector financiero	ASFI, Autoridad de Supervisión del Sistema Financiero
Acreditación	DTA, Dirección Técnica de Acreditación del IBMETRO

Lo que suelen exigir los clientes de la UE

Donde la ley calla, cuentan los certificados y las pruebas. Un exportador de castaña amazónica necesita certificados alimentarios [IFS](#), [BRCGS](#) o [FSSC 22000](#) y trazabilidad completa. A las empresas mineras se les pregunta por estándares ambientales y laborales, a menudo con referencia a [ISO 14001](#) y a las obligaciones europeas de diligencia debida en la cadena de suministro. El ganado, la soja y la madera de las tierras bajas quedan alcanzados por el [EUDR](#).

Los proveedores de servicios que tratan datos para clientes de la UE reciben cláusulas contractuales tipo, un cuestionario de seguridad y, con frecuencia, la pregunta por [ISO 27001](#). Una plataforma GRC como [Sightadel](#) ayuda a llevar políticas, riesgos y evidencias en un solo lugar cuando ninguna ley da la estructura.

En la evaluación de impacto de la transferencia, su cliente de la UE tiene que describir quién podría acceder a los datos en Bolivia y cómo los protege. Para eso le pregunta por ubicaciones de almacenamiento, cifrado, derechos de acceso, registros y el manejo de requerimientos de información de autoridades. Tenga esos datos listos por escrito. Si el registro de actividades de tratamiento y las medidas técnicas y organizativas ya están documentados en una plataforma como [Sightadel](#), la respuesta se arma a partir de lo que existe. Un documento que pueda entregar a varios clientes le ahorra semanas de coordinación.

Un punto de partida razonable para empresas bolivianas:

1. Aclare cuáles de sus clientes están en la UE y qué normas de la UE rigen para sus compras.
2. Redacte un esquema propio de protección de datos tomando como modelo el RGPD, con registro de actividades de tratamiento y reglas de supresión.
3. Fije un plazo de notificación de incidentes y defina quién notifica.
4. Para las exportaciones agrícolas y de madera, verifique si se aplica el EUDR y reúna los geodatos.
5. Elija el certificado que sus clientes piden con más frecuencia y planifique la auditoría con un organismo reconocido.

Sus brechas se las muestra el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

Bolivia es Estado Parte del Mercosur desde 2024. Depositó el instrumento de ratificación del Protocolo de Adhesión el 08/07/2024 en Asunción (Ley 1567 del 04/07/2024), y la adhesión entró en vigor 30 días después. Para incorporar la normativa del Mercosur y el Arancel Externo Común tiene un período de transición de hasta cuatro años. Bolivia no participa en el [Acuerdo UE-Mercosur](#), que se aplica de forma provisional desde el 01/05/2026 con Argentina, Brasil, Paraguay y Uruguay. Por lo tanto, sus ventajas arancelarias no rigen para las mercaderías bolivianas.

La Comisión señala que Bolivia podría adherirse al Acuerdo Comercial con Colombia, Perú y Ecuador. Mientras tanto, el SPG+ sigue siendo la vía de acceso al mercado de la UE.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. Para aprovechar la preferencia del SPG, los exportadores normalmente tienen que estar inscritos en el registro electrónico de exportadores registrados de la Comisión (REX) y emitir una declaración de origen en la factura. Su importador en la UE suele conocer el procedimiento y puede ayudarlo. Conserve las pruebas durante varios años, porque la aduana puede hacer controles posteriores. Como el SPG+ está sujeto a condiciones, conviene seguir los informes de la Comisión sobre su cumplimiento por parte de Bolivia.

<https://www.mercoeu.com/es/paises/bolivia>

PAÍS · ASOCIADO AL MERCOSUR

Chile: lo que esperan los clientes de la UE

Chile tiene la ley de ciberseguridad más cercana a NIS2 en la región y una nueva ley de protección de datos que debe entrar en vigor el 01/12/2026. Desde febrero de 2025 lo une a la UE un acuerdo comercial modernizado.

Panorama: comercio con la UE

Según la Comisión Europea, en 2025 las importaciones de la UE desde Chile fueron en un 40 % productos vegetales, en un 20 % productos minerales y en otro 20 % metales comunes. Detrás de esas cifras están la fruta y el vino del Valle Central, pero también el cobre de Antofagasta y el litio de Atacama. Vale aclarar que el cobre no está incluido en el [CBAM](#); el acero, el aluminio y los fertilizantes, en cambio, sí.

Santiago es además un polo importante de proveedores de TI, centros de datos y fintechs que también atienden a clientes en España y otros países de la UE.

Protección de datos: la Ley 21.719 frente al RGPD

La Ley 21.719 reforma a fondo la antigua ley de protección de datos, la Ley 19.628. Se publicó el 13/12/2024 en el Diario Oficial y entra en vigor el 01/12/2026. La ley incorpora muchos elementos del [RGPD \(Reglamento General de Protección de Datos\)](#): bases de licitud, derechos ampliados de los titulares, incluida la portabilidad, obligaciones para los encargados, reglas para las transferencias internacionales y la obligación de notificar vulneraciones de seguridad. Lo nuevo es una autoridad de control propia, la Agencia de Protección de Datos Personales, con facultades para aplicar multas.

Posible aplazamiento: el 31/08/2026, el Gobierno ingresó el proyecto de ley Boletín 18.623-07. Este postergaría la entrada en vigor al 01/12/2027 y ampliaría el consejo de la Agencia. Al 11/10/2026 no ha sido aprobado, por lo que sigue rigiendo el 01/12/2026.

Chile no tiene una decisión de adecuación de la UE. Sus clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia para enviar datos a Chile.

Ciberseguridad frente a NIS2

La Ley 21.663, Ley Marco de Ciberseguridad, se publicó en abril de 2024. La Agencia Nacional de Ciberseguridad (ANCI) funciona desde el 01/01/2025 y las demás disposiciones rigen desde el

01/03/2025. Al igual que [NIS2](#), la ley distingue dos grupos: los prestadores de servicios esenciales y los Operadores de Importancia Vital (OIV). Ambos tienen que notificar al CSIRT Nacional los incidentes con efectos significativos; los OIV tienen además obligaciones sobre sistemas de gestión, planes de continuidad y auditorías.

En los plazos, Chile es más estricto que la UE. La alerta temprana tiene que enviarse dentro de las tres horas; NIS2 la exige dentro de las 24 horas. Los detalles los regula el Reglamento de Reporte de Incidentes (Decreto 295/2024).

En el sector financiero rigen además las normas de la Comisión para el Mercado Financiero (CMF) sobre seguridad de la información y ciberseguridad y sobre la notificación de incidentes operacionales. Quien provee a bancos o aseguradoras europeos recibe, además, cláusulas de [DORA](#).

Plazos de notificación comparados

MOTIVO	CHILE	UE
Alerta temprana de ciberincidente	3 horas desde que se tiene conocimiento (Ley 21.663)	24 horas (art. 23 NIS2)
Actualización	72 horas; 24 horas para OIV con un servicio esencial afectado	72 horas
Informe final	15 días corridos desde la alerta temprana	un mes
Plan de acción OIV	como máximo 7 días corridos	sin equivalente
Vulneración de datos ante la autoridad	obligación de notificar según la Ley 21.719 desde su entrada en vigor	72 horas (art. 33 RGPD)

Quien cumple los plazos chilenos cumple también los de NIS2. Un proceso de notificación pensado para tres horas no necesita, entonces, una segunda versión para los clientes de la UE.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	Agencia de Protección de Datos Personales (nueva con la Ley 21.719)
Ciberseguridad	ANCI, Agencia Nacional de Ciberseguridad
CSIRT	CSIRT Nacional de la ANCI
Sector financiero	CMF, Comisión para el Mercado Financiero

ÁREA	ORGANISMO
Acreditación	INN, Instituto Nacional de Normalización

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del INN o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

A los exportadores de fruta y vino se les pregunta por inocuidad alimentaria, por lo general con certificados [IFS](#), [BRCGS](#) o [FSSC 22000](#) o GLOBALG.A.P. La madera y la celulosa quedan alcanzadas por el [EUDR](#). Ahí Chile está clasificado como país de riesgo bajo, de modo que la diligencia debida es simplificada, pero no prescindible. Las empresas mineras reciben preguntas sobre medio ambiente, derechos humanos y emisiones, a menudo con referencia a [ISO 14001](#).

A los proveedores de TI y centros de datos se les pregunta por [ISO 27001](#). Quien ya está alcanzado por la Ley 21.663 como OIV o prestador de servicios esenciales tiene armados el proceso de notificación y el sistema de gestión, y puede usarlos como prueba ante clientes de la UE. Si todavía no lo tiene, puede armarlo según ISO 27001 en una plataforma GRC como [Sightadel](#), que también cubre NIS2. Muchos clientes revisan además sus sistemas accesibles desde afuera. Con [veyrisk](#) usted mismo vigila esa superficie de ataque.

En el contrato, estos puntos suelen figurar en anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Para la evaluación de impacto de la transferencia, su cliente de la UE pregunta por ubicaciones de almacenamiento, accesos y cifrado. Con la Ley 21.719 y una autoridad de protección de datos propia, en adelante podrá remitirse a un marco legal más cercano al europeo.

Un punto de partida razonable para empresas chilenas:

1. Verifique si queda alcanzado por la Ley 21.663, como prestador de servicios esenciales o como OIV.
2. Prepárese para la Ley 21.719 como si el 01/12/2026 fuera seguro. Lo que haga para eso lo esperan de todos modos sus clientes de la UE.
3. Unifique en un solo flujo los procesos de notificación ante la ANCI, la nueva Agencia de Protección de Datos y sus clientes de la UE.

4. Para la madera, la celulosa y otros productos del EUDR, revise con su comprador la diligencia debida simplificada.
5. Para el acero, el aluminio y los fertilizantes, aclare qué datos de emisiones necesita su importador para el CBAM.

Un panorama rápido se lo da el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

Chile está asociado al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Tiene su propio marco de acuerdos con la UE: el Acuerdo Marco Avanzado y el Acuerdo Comercial Interino, ambos firmados el 13/12/2023. El Acuerdo Comercial Interino está en vigor desde el 01/02/2025 y reemplaza la parte comercial del Acuerdo de Asociación de 2002. Incluye, entre otros, capítulos sobre energía y materias primas y sobre desarrollo sostenible. Para la preferencia arancelaria necesita una declaración de origen.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. La mayor parte del comercio entre Chile y la UE está libre de aranceles. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en Chile. Para el litio y el cobre, el acuerdo contiene reglas propias sobre materias primas y energía. Su importador en la UE puede ayudarle a emitir correctamente la declaración de origen. Conserve las pruebas durante varios años, porque la aduana puede hacer controles posteriores.

Aun con el acuerdo, el EUDR, el CBAM y el RGPD se aplican sin cambios a las mercaderías y servicios chilenos.

<https://www.mercoeu.com/es/paises/chile>

PAÍS · ASOCIADO AL MERCOSUR

Colombia: lo que esperan los clientes de la UE

Colombia tiene un régimen de protección de datos consolidado y con una autoridad activa, pero no una ley de ciberseguridad. Con la UE rige un acuerdo comercial desde 2013.

Panorama: comercio con la UE

Colombia exporta a la UE sobre todo materias primas y productos agrícolas, entre ellos café del Huila y del Eje Cafetero, banano de Urabá, flores de corte de la Sabana de Bogotá, aguacate y carbón. La página de la Comisión no trae un desglose solo para Colombia. Para el conjunto de los países andinos, menciona para 2025 productos agrícolas (48,7 %), productos minerales (27,1 %) y pesca (13,5 %).

Además crece la exportación de servicios de TI. Equipos de Medellín, Bogotá y Cali desarrollan software y prestan soporte a clientes de España y otros países de la UE.

Protección de datos: la Ley 1581 frente al RGPD

La base es la Ley Estatutaria 1581 de 2012 con sus decretos reglamentarios (Decreto 1377/2013 y Decreto 886/2014, hoy compilados en el Decreto Único 1074/2015). La autoridad es la SIC (Superintendencia de Industria y Comercio), con una delegatura propia de protección de datos. La SIC realiza inspecciones e impone multas.

El derecho colombiano se apoya más en la autorización del titular que el [RGPD \(Reglamento General de Protección de Datos\)](#), que contempla varias bases legales del mismo rango. Las empresas a partir de cierto tamaño tienen que inscribir sus bases de datos en el Registro Nacional de Bases de Datos (RNBD). Allí también se reportan los incidentes de seguridad. Los responsables deben tener políticas escritas de tratamiento de la información, lo que en la práctica se acerca a un esquema de protección de datos según el RGPD.

Colombia no tiene una decisión de adecuación de la UE. Sus clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia. A la inversa, la SIC también controla las transferencias desde Colombia al exterior. Quien mueve datos en ambas direcciones tiene que tener en cuenta los dos regímenes.

Ciberseguridad frente a NIS2

Colombia no tiene una ley de ciberseguridad. La base son el documento de política CONPES 3995 de 2020, sobre confianza y seguridad digital, y el Decreto 338 de 2022, que regula la gobernanza de la seguridad digital. Hace años que se discute una agencia nacional de seguridad digital, pero no se ha creado. El equipo estatal de respuesta es ColCERT, del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Comparado con [NIS2](#), faltan obligaciones transversales de gestión de riesgos y plazos de notificación. El sector financiero está más regulado: la Superintendencia Financiera exige a los bancos y demás entidades vigiladas medidas de ciberseguridad y el reporte de incidentes (Circular Externa 007 de 2018, hoy parte de la Circular Básica Jurídica).

Para los proveedores de clientes europeos, las obligaciones vienen del contrato: cláusulas de NIS2 sobre la cadena de suministro, [DORA](#) si el cliente es del sector financiero y el [Reglamento de Ciberresiliencia \(CRA\)](#) para productos conectados.

Plazos de notificación comparados

MOTIVO	COLOMBIA	UE
Violación de datos ante la autoridad	15 días hábiles desde que se tiene conocimiento, a la SIC a través del RNBD	72 horas (art. 33 RGPD)
Ciberincidente significativo	sin ley general; sector financiero según las normas de la Superintendencia Financiera	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

El plazo colombiano es bastante más largo que el europeo. Si trata datos por encargo de un cliente de la UE, para usted rige el plazo del contrato, por lo general de 24 a 48 horas, para que el cliente pueda cumplir sus 72 horas.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	SIC, Superintendencia de Industria y Comercio
Ciberseguridad, CSIRT	MinTIC con ColCERT
Sector financiero	Superintendencia Financiera de Colombia
Acreditación	ONAC, Organismo Nacional de Acreditación de Colombia

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del ONAC o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

Los exportadores de café, cacao y aceite de palma tienen que cumplir el [EUDR](#): geodatos de las fincas, prueba de producción libre de deforestación después del 31/12/2020 y prueba de producción legal. Colombia está clasificada como país de riesgo estándar. Para una cooperativa del Huila con cientos de pequeños productores, reunir los polígonos es el mayor esfuerzo. A los exportadores de banano y flores se les piden certificados como GLOBALG.A.P. o [normas alimentarias](#).

Los proveedores de TI reciben cláusulas contractuales tipo, un cuestionario de seguridad y, a menudo, la pregunta por [ISO 27001](#). Si quiere implementar un sistema de gestión de seguridad de la información, puede llevar políticas, riesgos y evidencias en una plataforma GRC como [Sightadel](#). Para las preguntas del cuestionario sobre sistemas accesibles desde internet, un análisis externo como el de [veyrisk](#) le da una respuesta con evidencia.

En el contrato, estos puntos suelen figurar como anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Para la evaluación de impacto de la transferencia, su cliente de la UE pregunta por ubicaciones de almacenamiento, accesos y cifrado. Como en Colombia ya lleva políticas de tratamiento de la información e inscribe sus bases de datos en el RNBD, una parte de las respuestas ya está documentada.

Un punto de partida razonable para empresas colombianas:

1. Aclare cuáles de sus clientes están en la UE y qué normas se les aplican.
2. Compare sus políticas según la Ley 1581 con los requisitos del RGPD, sobre todo en bases legales y plazos de supresión.
3. Reduzca su plazo interno de notificación de incidentes muy por debajo de los 15 días hábiles de la SIC.
4. Para café, cacao y aceite de palma, reúna los geodatos de todas las parcelas, también los de sus proveedores.
5. Evalúe si un certificado ISO 27001 o una norma alimentaria responde muchas preguntas individuales de una sola vez.

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

Acuerdo con la UE

Colombia está asociada al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Con la UE rige el Acuerdo Comercial con Colombia, Perú y Ecuador, que se aplica de forma provisional con Colombia desde el 01/08/2013. Para la preferencia arancelaria necesita una prueba de origen. El acuerdo incluye un capítulo sobre comercio y desarrollo sostenible con referencias a las normas fundamentales del trabajo de la OIT y a los acuerdos ambientales internacionales.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. Muchos productos agrícolas e industriales están libres de aranceles desde hace años; para algunos rigen contingentes o reglas transitorias. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en el país. Su importador en la UE puede ayudarle a emitir correctamente la prueba de origen. Conserve los documentos durante varios años, porque la aduana puede hacer controles posteriores.

El derecho de la UE, como el EUDR, el CBAM y el RGPD, se aplica a las mercancías y servicios colombianos con independencia del acuerdo.

<https://www.mercoeu.com/es/paises/colombia>

PAÍS · ASOCIADO AL MERCOSUR

Perú: lo que esperan los clientes de la UE

En 2025, Perú modernizó su régimen de protección de datos y exige notificar los incidentes de seguridad dentro de las 48 horas. Desde fines de 2025, los servicios digitales de sectores clave tienen además la obligación de notificar al centro nacional de seguridad digital.

Panorama: comercio con la UE

Perú exporta a la UE sobre todo productos mineros y agrícolas: concentrados de cobre y zinc de los Andes, arándanos, paltas y uvas de la costa, café de Cajamarca y Junín, además de harina de pescado. La Comisión publica las cifras solo para el conjunto de los países andinos. En 2025, el 48,7 % correspondió a productos agrícolas, el 27,1 % a productos minerales y el 13,5 % a la pesca.

Para los exportadores de café y cacao, el [EUDR](#) es la obligación nueva más importante. A las empresas mineras se les pregunta sobre todo por medio ambiente, condiciones laborales y emisiones.

Protección de datos: la Ley 29733 frente al RGPD

La base es la Ley Nº 29733 de Protección de Datos Personales, de 2011. El nuevo reglamento, Decreto Supremo Nº 016-2024-JUS, está vigente desde el 30/03/2025 y reemplaza al reglamento anterior de 2013. Acerca bastante el derecho peruano al [RGPD \(Reglamento General de Protección de Datos\)](#): oficial de datos personales para ciertos titulares de bancos de datos, obligaciones en los flujos transfronterizos, reglas para los encargados del tratamiento y, sobre todo, un plazo fijo para notificar incidentes de seguridad. La autoridad es la Autoridad Nacional de Protección de Datos Personales (ANPD), del Ministerio de Justicia y Derechos Humanos.

Con 48 horas, el plazo de notificación es más corto que las 72 horas del RGPD. Los especialistas interpretan de distinta manera en qué momento exacto corresponde notificar. Ante la duda, mejor notifique. Un proveedor peruano que trata datos por encargo de un cliente de la UE tiene que ser rápido, entonces, tanto con su cliente como con la ANPD.

Perú no tiene una decisión de adecuación de la UE. Los clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia.

Ciberseguridad frente a NIS2

Con la Ley Nº 30999 (Ley de Ciberdefensa) de 2019, Perú tiene una ley de ciberdefensa del Estado. Regula las funciones de las Fuerzas Armadas y del Estado, no las obligaciones de las empresas. Una ley de ciberseguridad que, como NIS2, imponga obligaciones a las empresas no existe; en el Congreso solo hay proyectos. La base es el Marco de Confianza Digital (Decreto de Urgencia Nº 007-2020) junto con la Ley de Gobierno Digital (Decreto Legislativo 1412). Su reglamento, el Decreto Supremo Nº 126-2025-PCM, se publicó en noviembre de 2025. Según este, los proveedores de servicios digitales en sectores como finanzas, servicios básicos, salud, transporte, acceso a internet y educación tienen que notificar los incidentes críticos al Centro Nacional de Seguridad Digital (CNSD).

El enfoque se parece al de [NIS2](#): obligaciones para sectores clave, un punto central de notificación y plazos cortos. NIS2 va más allá, por ejemplo en las obligaciones de gestión de riesgos, de cadena de suministro y de responsabilidad personal de la dirección. Los bancos y las aseguradoras tienen además sus propias exigencias de seguridad de la información y ciberseguridad fijadas por la SBS.

Para los proveedores de clientes europeos se suman los requisitos contractuales: cláusulas de NIS2 sobre la cadena de suministro, [DORA](#) si el cliente es del sector financiero y el [Reglamento de Ciberresiliencia \(CRA\)](#) para productos conectados.

Plazos de notificación comparados

MOTIVO	PERÚ	UE
Violación de datos ante la autoridad	48 horas desde que se tiene conocimiento, ante la ANPD (DS 016-2024-JUS)	72 horas (art. 33 RGPD)
Incidente crítico en servicios digitales	48 horas ante el CNSD (DS 126-2025-PCM)	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Un incidente con datos personales puede dar lugar a las dos notificaciones, ante la ANPD y ante el CNSD. Téngalo previsto en su proceso, con un responsable claro para cada notificación.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	ANPD, Ministerio de Justicia y Derechos Humanos
Seguridad digital	Secretaría de Gobierno y Transformación Digital (PCM)
CSIRT	Centro Nacional de Seguridad Digital con PeCERT

ÁREA	ORGANISMO
Sector financiero	SBS, Superintendencia de Banca, Seguros y AFP
Acreditación	INACAL, Instituto Nacional de Calidad

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del INACAL o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

Un exportador de café de Junín necesita, para el EUDR, los geodatos de todas las parcelas de sus proveedores y la prueba de que allí no hubo deforestación después del 31/12/2020. Perú está clasificado como país de riesgo estándar. A los exportadores de fruta se les pide [IFS](#), [BRCGS](#) o [FSSC 22000](#) y GLOBALG.A.P.; a las empresas mineras, con frecuencia, [ISO 14001](#).

Los proveedores de TI y de outsourcing reciben cláusulas contractuales tipo, cuestionarios de seguridad y la pregunta por [ISO 27001](#). Las políticas, los riesgos y las evidencias que piden esos cuestionarios se pueden llevar en una plataforma GRC como [Sightadel](#). Muchos clientes de la UE revisan también qué sistemas de sus proveedores están expuestos en internet. Con [veyrisk](#) usted ve esa superficie de ataque antes de que el cliente pregunte.

En el contrato, estos puntos suelen figurar en anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Para la evaluación de impacto de la transferencia, su cliente de la UE pregunta por ubicaciones de almacenamiento, accesos y cifrado. Aquí le ayuda que el derecho peruano, con el nuevo reglamento, ya contemple un plazo de notificación corto y obligaciones para los encargados.

Un punto de partida razonable para empresas peruanas:

1. Verifique si, como proveedor de servicios digitales, queda alcanzado por el DS 126-2025-PCM.
2. Compare su documentación según el DS 016-2024-JUS con los requisitos del RGPD.
3. Arme un proceso de notificación que atienda a la ANPD, al CNSD y a sus clientes de la UE dentro del mismo plazo.
4. Para café y cacao, reúna los geodatos de todas las parcelas, también los de sus proveedores.

5. Verifique qué certificado piden sus clientes con más frecuencia y planifique la auditoría con un organismo reconocido.

Un primer panorama se lo da el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

Perú está asociado al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Con la UE rige el Acuerdo Comercial con Colombia, Perú y Ecuador, que se aplica de forma provisional con Perú desde el 01/03/2013. Para la preferencia arancelaria necesita una prueba de origen. El capítulo sobre comercio y desarrollo sostenible remite a las normas fundamentales del trabajo de la OIT y a los acuerdos ambientales internacionales.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. Muchos productos agrícolas e industriales están libres de aranceles desde hace años; para algunos rigen contingentes o reglas transitorias. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en el país. Su importador en la UE puede ayudarle a emitir correctamente la prueba de origen. Conserve los documentos durante varios años, porque la aduana puede hacer controles posteriores.

El EUDR, el CBAM y el RGPD se aplican a las mercancías y servicios peruanos con independencia del acuerdo.

<https://www.mercoeu.com/es/paises/peru>

PAÍS · ASOCIADO AL MERCOSUR

Ecuador: lo que esperan los clientes de la UE

Ecuador tiene desde 2021 una ley de protección de datos inspirada en el modelo europeo y, desde mayo de 2026, una ley para el fortalecimiento de la ciberseguridad. Con la UE lo une un acuerdo comercial desde 2017.

Panorama: comercio con la UE

Ecuador envía a Europa sobre todo alimentos: banano de El Oro y Los Ríos, camarón del golfo de Guayaquil, atún en conserva de Manta, cacao y flores de corte de la Sierra. La Comisión publica cifras solo para el conjunto de los países andinos. En 2025, el 48,7 % correspondió a productos agrícolas, el 27,1 % a productos minerales y el 13,5 % a la pesca, un rubro en el que Ecuador es especialmente fuerte.

Para los exportadores de cacao y aceite de palma rige el [EUDR](#). Las empresas pesqueras y alimentarias necesitan además la habilitación de la UE para alimentos de origen animal y certificados alimentarios sólidos.

Protección de datos: la LOPDP frente al RGPD

La Ley Orgánica de Protección de Datos Personales (LOPDP) se publicó en mayo de 2021 en el Registro Oficial. Tras un período de transición de dos años, desde mayo de 2023 rigen también las sanciones. El reglamento es el Decreto Ejecutivo 904 de 2023. La autoridad de control es la Superintendencia de Protección de Datos Personales (SPDP).

La LOPDP sigue de cerca al [RGPD \(Reglamento General de Protección de Datos\)](#): bases de legitimación, derechos de los titulares, delegados de protección de datos, evaluaciones de impacto, obligaciones de los encargados y reglas para las transferencias internacionales. Quien conoce el RGPD se orienta rápido.

La diferencia está en el plazo de notificación de vulneraciones: el art. 43 de la LOPDP exige notificar a la SPDP a más tardar cinco días después de la vulneración. Los encargados tienen que informar al responsable dentro de los dos días. La notificación se hace mediante un sistema electrónico de la SPDP.

Ecuador no tiene una decisión de adecuación de la UE. Sus clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia.

Ciberseguridad frente a NIS2

Desde el 22/05/2026 rige la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada en el Registro Oficial. Su objetivo declarado es proteger la infraestructura crítica y asegurar la continuidad de los servicios esenciales. Crea un Sistema Nacional de Ciberseguridad y reforma siete leyes vigentes, entre ellas la LOPDP y la ley de telecomunicaciones. En el centro están las entidades públicas y los operadores de infraestructura crítica.

El enfoque se parece al de [NIS2](#), que apunta a entidades esenciales e importantes de 18 sectores. Si su empresa está alcanzada, qué obligaciones de gestión de riesgos rigen y en qué plazo hay que notificar los incidentes es algo que conviene verificar en el texto de la ley publicado en el Registro Oficial y en su normativa de aplicación. Una empresa que ya trabaja según [ISO 27001](#) va a tener cubierta la mayoría de los requisitos.

Para los proveedores de clientes europeos rigen, con independencia de eso, los requisitos contractuales: cláusulas de NIS2 sobre la cadena de suministro, [DORA](#) si el cliente es del sector financiero y el [Reglamento de Ciberresiliencia \(CRA\)](#) para productos conectados.

Plazos de notificación comparados

MOTIVO	ECUADOR	UE
Violación de datos ante la autoridad	a más tardar 5 días después de la vulneración, ante la SPDP (art. 43 LOPDP)	72 horas (art. 33 RGPD)
Encargado al responsable	2 días	sin dilación indebida (art. 33, apdo. 2 RGPD)
Ciberincidente significativo	ley vigente desde el 22/05/2026; verificar plazo y organismo receptor en el texto del Registro Oficial	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Si trata datos por encargo de un cliente de la UE, rige el plazo del contrato, por lo general de 24 a 48 horas. Los dos días que la LOPDP da a los encargados normalmente no alcanzan para eso.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO

Protección de datos	SPDP, Superintendencia de Protección de Datos Personales
CSIRT	EcuCERT de la ARCOTEL
Sector financiero	Superintendencia de Bancos
Acreditación	SAE, Servicio de Acreditación Ecuatoriano

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del SAE o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Qué organismo recibe las notificaciones bajo la nueva ley de ciberseguridad conviene verificarlo directamente en el texto de la ley o con su ente de control sectorial.

Lo que suelen exigir los clientes de la UE

Un camaronero de El Oro que vende a un mayorista en España necesita la habilitación de su establecimiento para el mercado de la UE, trazabilidad hasta la piscina y, por lo general, un certificado [IFS](#), [BRCGS](#) o [FSSC 22000](#). A los exportadores de banano y flores se les pide GLOBALG.A.P. Los exportadores de cacao tienen que entregar, para el EUDR, los geodatos de las parcelas y la prueba de producción libre de deforestación después del 31/12/2020. Ecuador está clasificado como país de riesgo estándar.

Los proveedores de TI reciben cláusulas contractuales tipo, cuestionarios de seguridad y la pregunta por [ISO 27001](#). Quien implementa un sistema de gestión según ISO 27001 puede llevar políticas, riesgos y evidencias en una plataforma GRC como [Sightadel](#). Para las preguntas sobre sistemas accesibles desde internet sirve un análisis externo, por ejemplo con [veyrisk](#), cuyo informe puede adjuntar a la respuesta.

En el contrato, estos puntos suelen figurar en anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Para la evaluación de impacto de la transferencia, su cliente de la UE pregunta por ubicaciones de almacenamiento, accesos y cifrado. La LOPDP le da una buena base para eso, porque adopta muchos conceptos y obligaciones del RGPD.

Un punto de partida razonable para empresas ecuatorianas:

1. Verifique si queda alcanzado por la ley de ciberseguridad de 2026.

2. Compare su documentación según la LOPDP con los requisitos del RGPD. Las brechas suelen ser pequeñas.
3. Reduzca su plazo interno de notificación de incidentes muy por debajo de los cinco días de la LOPDP.
4. Para cacao y aceite de palma, reúna los geodatos de todas las parcelas, también los de sus proveedores.
5. Mantenga al día las habilitaciones, la trazabilidad y los certificados alimentarios para camarón, atún y banano.

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

Acuerdo con la UE

Ecuador está asociado al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Se adhirió al Acuerdo Comercial de la UE con Colombia y Perú, que se aplica desde el 01/01/2017. Para la preferencia arancelaria necesita una prueba de origen. El acuerdo incluye un capítulo sobre comercio y desarrollo sostenible con referencias a las normas fundamentales del trabajo de la OIT y a los acuerdos ambientales internacionales.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. Muchos productos agrícolas e industriales están libres de aranceles desde hace años; para algunos rigen contingentes o reglas transitorias. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en el país. Su importador en la UE puede ayudarle a emitir correctamente la prueba de origen. Conserve los documentos durante varios años, porque la aduana puede hacer controles posteriores.

El EUDR, el CBAM y el RGPD se aplican a las mercancías y servicios ecuatorianos con independencia del acuerdo.

<https://www.mercoeu.com/es/paises/ecuador>