

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.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
Ley 18.331 (2008), Ley 19.670	sí, desde 2012	UE-Mercosur, provisional desde 01/05/2026	Ley 20.212 art. 78 y ss., Decreto 66/025

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
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 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.

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

FAQ

¿Necesitan los clientes de la UE cláusulas contractuales tipo para Uruguay?

No. Uruguay tiene una decisión de adecuación desde 2012 (2012/484/UE), confirmada en 2024.

¿En cuánto tiempo hay que notificar una violación de datos en Uruguay?

Dentro de las 72 horas desde que se tiene conocimiento, ante la URCDP (Decreto 64/020). Coincide con el plazo del RGPD.

¿Quién tiene que notificar ciberincidentes en Uruguay?

Los organismos públicos y los operadores privados de sectores críticos, dentro de las 24 horas, ante el CERTuy (Ley 20.212, Decreto 66/025).

¿Ayuda el Marco de Ciberseguridad con ISO 27001?

Sí, los controles se superponen mucho. Pero no reemplaza un certificado. Más información en la página sobre [ISO 27001](#).

¿Qué herramienta ayuda con ISO 27001 y DORA desde Uruguay?

[Sightadel](#) cubre ISO 27001 y DORA, entre otros marcos, y lo elaborado para uno se aprovecha para el otro. Se desarrolla y se aloja en Alemania. Para la superficie de ataque externa, que muchos clientes revisan por su cuenta, puede ver cómo luce un [informe de veyrisk](#).

Fuentes · Actualizado: 11 de octubre de 2026

Ley 18.331, IMPO: <https://www.impo.com.uy/bases/leyes/18331-2008>

Decreto 64/020, IMPO: <https://www.impo.com.uy/bases/decretos/64-2020>

Ley 20.212, art. 78, IMPO: <https://www.impo.com.uy/bases/leyes/20212-2023/78>

Decreto 66/025, IMPO: <https://www.impo.com.uy/bases/decretos/66-2025>

URCDP: <https://www.gub.uy/unidad-reguladora-control-datos-personales/>

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

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