

PAÍS · MERCOSUL

Uruguai: o que os clientes da UE esperam

O Uruguai tem a legislação de proteção de dados mais avançada do Mercosul e, desde 2012, uma decisão de adequação da UE. Para setores críticos, incidentes cibernéticos precisam ser notificados em até 24 horas.

PROTEÇÃO DE DADOS	ADEQUAÇÃO DA UE	ACORDO COM A UE	CIBERSEGURANÇA
Ley 18.331 (2008), Ley 19.670	sim, desde 2012	UE-Mercosul, provisório desde 01/05/2026	Ley 20.212 art. 78 e seguintes, Decreto 66/025

Visão geral: comércio com a UE

Segundo a Comissão Europeia, mais da metade das importações da UE vindas do Uruguai em 2025 foi de celulose e papel (52 %). Em seguida vêm produtos de origem animal (21 %), sobretudo carne bovina, e produtos vegetais (11 %). Fábricas de celulose às margens do Rio Uruguai e frigoríficos do interior são, portanto, diretamente afetados pelo [EUDR](#), que abrange madeira e gado.

Ao mesmo tempo, Montevidéu é um dos polos de software mais importantes da América Latina. Muitas empresas de lá desenvolvem para clientes na Espanha, na Alemanha ou na Escandinávia e tratam dados pessoais vindos da UE.

Proteção de dados: a Ley 18.331 comparada ao RGPD

A Ley 18.331 de proteção de dados pessoais é de 2008, e seu regulamento é o Decreto 414/009. Com a Ley 19.670, de 2018, e o Decreto 64/020, o Uruguai aproximou sua legislação do [RGPD](#) ([Regulamento Geral sobre a Proteção de Dados](#)): a lei vale também para controladores no exterior que tratam dados de pessoas no Uruguai, há obrigação de notificar incidentes com dados, e determinadas entidades precisam nomear um encarregado de dados. A autoridade de supervisão é a URCDP (Unidad Reguladora y de Control de Datos Personales), ligada à AGESIC.

A UE reconheceu o Uruguai como adequado em 2012, com a Decisão de Execução 2012/484/UE, e confirmou isso no relatório da Comissão de 15/01/2024. O Uruguai também ratificou a Convenção 108+ do Conselho da Europa. Seus clientes na UE podem, portanto, transferir dados para o Uruguai sem cláusulas contratuais padrão.

Para operadores, a adequação muda pouco na papelada: o contrato do art. 28 do RGPD, a lista de subcontratados e a comprovação das medidas técnicas e organizacionais continuam obrigatórios.

Cibersegurança comparada à NIS2

O Uruguai é um dos poucos países da região com obrigações legais de cibersegurança fora do setor financeiro. A Ley 20.212 (Rendición de Cuentas 2022), no art. 78 e nos artigos seguintes, obriga órgãos públicos e operadores privados de setores críticos a notificar incidentes de segurança em até 24 horas. O Decreto 66/025 regula a implementação: notificação ao CERTuy, nomeação de responsáveis pela segurança, guarda de registros e aplicação do Marco de Ciberseguridad, um referencial nacional com controles parecidos com os da ISO 27001.

Em comparação com a [NIS2](#), o grupo de obrigados é menor. Na UE, a NIS2 abrange também empresas de médio porte de 18 setores, entre eles a produção de alimentos e os serviços digitais. No Uruguai, a obrigação recai sobre os setores críticos. Com 24 horas, porém, a primeira notificação é tão rápida quanto o alerta inicial da NIS2.

Para fornecedores de clientes europeus, somam-se as exigências contratuais: cláusulas da NIS2 sobre a cadeia de suprimentos, o [DORA](#) no caso de clientes financeiros e o [Cyber Resilience Act](#) para produtos com elementos digitais.

Prazos de notificação comparados

SITUAÇÃO	URUGUAI	UE
Incidente com dados, aviso à autoridade	72 horas a partir do conhecimento, à URCDP (Decreto 64/020, art. 4)	72 horas (art. 33 do RGPD)
Primeiras medidas após um incidente com dados	iniciar em até 24 horas (Decreto 64/020, art. 3)	sem prazo próprio
Incidente cibernético, setores críticos	24 horas ao CERTuy (Ley 20.212, Decreto 66/025)	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

Os prazos para incidentes com dados são iguais no Uruguai e na UE. Um processo que atenda aos dois é, portanto, simples de montar.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	URCDP, na AGESIC
Cibersegurança, CSIRT	AGESIC com o CERTuy
Setor financeiro	BCU, Banco Central del Uruguay
Acreditação	OUA, Organismo Uruguayo de Acreditación

Para certificados, importa menos onde está o organismo certificador e mais quem o acreditou. Pergunte antes da contratação se a acreditação pelo OUA ou por um órgão estrangeiro está coberta pelo acordo internacional de reconhecimento da Global ACI (desde 01/01/2026 sucessora do IAF e do ILAC; as creditações existentes continuam reconhecidas). Nesse caso, o certificado costuma ser aceito por clientes da UE. Alguns grupos empresariais ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

O que os clientes da UE costumam exigir

Uma software house de Montevideú que desenvolve para um banco em Madri recebe um questionário de segurança, um contrato nos termos do art. 28 do RGPD e cláusulas do DORA sobre direitos de auditoria e planos de saída. Muitas vezes se espera um certificado [ISO 27001](#). Quem já trabalha conforme o Marco de Ciberseguridad tem boa parte dos controles implementada. Para a ISO 27001 e o DORA, o [Sightadel](#) conduz você pelos requisitos com modelos, tarefas e comprovações.

Muitos clientes da UE também verificam a superfície de ataque visível de fora dos seus prestadores. Com o [veyrisk](#), você vê os mesmos achados e pode corrigi-los antes que o cliente pergunte.

Para o EUDR, exportadores de celulose e madeira precisam dos dados de geolocalização das plantações e da comprovação de origem livre de desmatamento. Exportadores de carne precisam das mesmas informações para as áreas de pastagem, além de certificações de alimentos [IFS](#), [BRCGS](#) ou [FSSC 22000](#).

No contrato, essas exigências costumam aparecer como anexos: contrato de tratamento de dados, medidas técnicas e organizacionais, prazos de notificação, direitos de auditoria e uma lista de subcontratados. Graças à adequação, as cláusulas contratuais padrão não são necessárias. Mas se você usa prestadores em países sem adequação, por exemplo uma equipe de suporte na Ásia, seu cliente da UE vai querer saber como essa transferência está protegida.

Um bom ponto de partida para empresas do Uruguai:

1. Verifique se sua empresa pertence a um setor crítico nos termos da Ley 20.212. Nesse caso, a notificação ao CERTuy em 24 horas já vale para você.
2. Compare sua documentação segundo a Ley 18.331 e a Ley 19.670 com os requisitos do RGPD. As lacunas costumam ser pequenas.
3. Monte um processo único de notificação para a URCDP, o CERTuy e seus clientes da UE.
4. Avalie até que ponto seus controles segundo o Marco de Ciberseguridad já cobrem os requisitos da ISO 27001.
5. Para exportações de madeira, celulose e carne, reúna os dados de geolocalização exigidos pelo EUDR.

O [Diagnóstico UE](#) gratuito mostra onde você está.

Acordo com a UE

O [acordo UE-Mercosul](#) foi assinado em 17/01/2026 em Assunção e ratificado pelo Uruguai em fevereiro de 2026. Desde 01/05/2026, a parte comercial é aplicada provisoriamente entre a UE e Uruguai, Argentina, Brasil e Paraguai. A preferência tarifária exige uma declaração de origem. O acordo de parceria mais amplo ainda está em ratificação.

Na prática, isso significa: verifique para cada mercadoria a alíquota, o cronograma de redução tarifária e a regra de origem. Você encontra essas informações no portal Access2Markets da Comissão Europeia, organizadas por código de mercadoria. No caso de produtos processados, a regra de origem define se houve agregação de valor suficiente no Mercosul. Para alguns produtos agrícolas valem cotas tarifárias, ou seja, quantidades limitadas com tarifa preferencial. Seu importador na UE muitas vezes conhece essas regras melhor do que você e pode ajudar a colocar a declaração de origem corretamente na fatura. Guarde as comprovações de origem por vários anos, porque a alfândega pode verificar depois.

Apesar do acordo, o direito da UE vale integralmente, inclusive EUDR, CBAM e RGPD.

FAQ

Clientes da UE precisam de cláusulas contratuais padrão para o Uruguai?

Não. O Uruguai tem uma decisão de adequação desde 2012 (2012/484/UE), confirmada em 2024.

Em quanto tempo um incidente com dados precisa ser notificado no Uruguai?

Em até 72 horas a partir do conhecimento, à URCDP (Decreto 64/020). É o mesmo prazo do RGPD.

Quem precisa notificar incidentes cibernéticos no Uruguai?

Órgãos públicos e operadores privados de setores críticos, em até 24 horas, ao CERTuy (Ley 20.212, Decreto 66/025).

O Marco de Ciberseguridad ajuda com a ISO 27001?

Sim, os controles se sobrepõem bastante. Mas ele não substitui um certificado. Mais na página sobre a [ISO 27001](#).

Qual ferramenta ajuda a responder ao questionário de segurança de um cliente da UE?

O [veyrisk](#) verifica de fora sua superfície de ataque e gera um relatório que serve como comprovação para ISO 27001 e NIS2. Para os demais controles, o [Sightadel](#) reúne tarefas, comprovações e a preparação da auditoria. Ele é hospedado na Alemanha, e os dados ficam na UE.

Fontes · Atualizado em: 11 de outubro 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/>

Comissão Europeia: decisões de adequação: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Comissão Europeia, DG Comércio: Uruguai: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/uruguay_en

Informações gerais, sem caráter de consultoria jurídica. Valem os textos oficiais.

COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



Sightadel

O Sightadel conduz sua equipe por a NIS2: modelos, tarefas, evidências e preparação para auditoria em um só lugar. Desenvolvido e hospedado na Alemanha, com pacote de consultoria opcional.

[Conhecer o Sightadel →](#)



O veyrisk mostra o que um atacante enxerga da sua empresa por fora: serviços abertos, certificados, vulnerabilidades conhecidas. Você pode apresentar o relatório a clientes europeus e auditores.

[Conhecer o veyrisk →](#)



Valar é um firewall de hardware com software da neonotu. Protege escritórios e unidades e gera os registros exigidos pela NIS2 e pela ISO 27001.

[Conhecer o Valar →](#)

Sightadel, veyrisk e Valar são produtos da neonotu GmbH, empresa que opera o MercoEU.

O que disso se aplica à sua empresa?

O Diagnóstico UE gratuito mostra isso por setor e país em 10 minutos.

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