

RELATÓRIO POR PAÍS

América do Sul e UE: comparação jurídica

Proteção de dados, cibersegurança, prazos de notificação, autoridades e acordos comerciais de Argentina, Brasil, Paraguai, Uruguai, Bolívia, Chile, Colômbia, Peru e Equador.

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

Conteúdo

1. Seu país diante do direito da UE
2. Argentina: o que os clientes da UE esperam
3. Brasil: o que os clientes da UE esperam
4. Paraguai: o que os clientes da UE esperam
5. Uruguai: o que os clientes da UE esperam
6. Bolívia: o que os clientes da UE esperam
7. Chile: o que os clientes da UE esperam
8. Colômbia: o que os clientes da UE esperam
9. Peru: o que os clientes da UE esperam
10. Equador: o que os clientes da UE esperam

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

PAÍSES · VISÃO GERAL

Seu país diante do direito da UE

Para cada um dos nove países mostramos em que pé está a legislação local, o que a diferencia do RGPD (Regulamento Geral sobre a Proteção de Dados) e da NIS2 e qual acordo com a UE está em vigor.

Os nove países em um quadro

PAÍS	LEI DE PROTEÇÃO DE DADOS	LEI DE CIBERSEGURANÇA	ADEQUAÇÃO À UE	ACORDO COMERCIAL COM A UE
Argentina	Ley 25.326 (2000), reforma em discussão no Congresso	nenhuma	sim (2003)	UE-Mercosul, provisório desde 01/05/2026
Brasil	LGPD, Lei 13.709/2018	nenhuma, projeto PL 4.752/2025	sim (desde 01/2026)	UE-Mercosul, provisório desde 01/05/2026
Paraguai	Ley 7593/2025, plena a partir do fim de 11/2027	nenhuma	não	UE-Mercosul, provisório desde 01/05/2026
Uruguai	Ley 18.331 (2008), Ley 19.670	Ley 20.212, art. 78 e seguintes, Decreto 66/025	sim (2012)	UE-Mercosul, provisório desde 01/05/2026
Bolívia	nenhuma	nenhuma	não	nenhum; preferências tarifárias pelo SPG+
Chile	Ley 21.719, em vigor a partir de 01/12/2026 (adiamento proposto)	Ley 21.663 (2024)	não	Acordo comercial provisório desde 01/02/2025
Colômbia	Ley 1581 de 2012	nenhuma, Decreto 338/2022	não	Acordo comercial desde 2013
Peru	Ley 29733, DS 016-2024-JUS	marco via DU 007-2020 e DS 126-2025-PCM	não	Acordo comercial desde 2013

PAÍS	LEI DE PROTEÇÃO DE DADOS	LEI DE CIBERSEGURANÇA	ADEQUAÇÃO À UE	ACORDO COMERCIAL COM A UE
Equador	LOPDP (2021)	Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026)	não	Acordo comercial desde 2017

O que a adequação muda na prática

Para a Argentina, o Uruguai e, desde janeiro de 2026, também o Brasil, a UE reconheceu que a proteção de dados é equivalente à europeia. Seus clientes na UE podem transferir dados para esses países sem assinar cláusulas contratuais padrão. Para os outros seis países, eles precisam dessas cláusulas e de uma avaliação de impacto da transferência. O contrato de tratamento de dados como operador exigido pelo [RGPD](#) continua necessário nos nove países, inclusive no Brasil.

Cibersegurança: poucas leis, muitos contratos

O país mais próximo da [NIS2](#) é o Chile, onde um alerta precoce já é exigido em três horas. O Uruguai exige dos setores críticos uma notificação em até 24 horas. O Equador tem lei própria desde maio de 2026, e o Peru regula as notificações de serviços digitais por decreto. Nos demais países, valem sobretudo as normas dos supervisores bancários.

Para fornecedores, a lei local é só uma parte da história. Os clientes na UE repassam por contrato as obrigações da NIS2, da [DORA](#) e do [Cyber Resilience Act](#), seja qual for o país da sua empresa. Para organizar essas obrigações e as comprovações, você pode usar uma plataforma GRC como o [Sightadel](#), que traz NIS2, DORA e ISO 27001 como marcos próprios.

Acordos e cadeia de suprimentos

O [Acordo UE-Mercosul](#) é aplicado provisoriamente desde 01/05/2026 com Argentina, Brasil, Paraguai e Uruguai. A Bolívia é membro do Mercosul, mas não faz parte do acordo. Chile, Colômbia, Peru e Equador têm acordos próprios. Nenhum deles dispensa a [EUDR](#) ou o [CBAM](#).

Para saber onde sua empresa está hoje, faça o [Diagnóstico UE](#) gratuito.

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

PAÍS · MERCOSUL

Argentina: o que os clientes da UE esperam

Desde 2003, a UE reconhece a Argentina como país com nível adequado de proteção de dados. A lei que sustenta esse reconhecimento é de 2000, e uma reforma tramita no Congresso. Uma lei de cibersegurança não existe.

Visão geral: comércio com a UE

Segundo a Comissão Europeia, cerca de dois terços das exportações argentinas para a UE em 2025 foram produtos agrícolas, sobretudo oleaginosas e proteaginosas como a soja e as rações feitas a partir dela. Produtos químicos responderam por 13,7 %, combustíveis e produtos de mineração por 6,7 %. Quem vende farelo de soja de Rosario ou carne bovina do Pampa para a Europa precisa, portanto, olhar primeiro para o [EUDR](#).

A Argentina também tem um setor de software forte. Equipes de desenvolvimento em Buenos Aires, Córdoba e Mendoza trabalham há anos para clientes na Espanha, na Alemanha e na Holanda. Para elas, o foco está na proteção de dados e na segurança da informação.

Proteção de dados: a Ley 25.326 comparada ao RGPD

A base é a Ley 25.326 de proteção de dados pessoais, de 2000, regulamentada pelo Decreto 1558/2001. A autoridade competente é a AAIP (Agencia de Acceso a la Información Pública). A lei prevê consentimento, limitação de finalidade, direitos de acesso e de exclusão e um registro de bancos de dados. Muito do que o [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#) desenvolveu depois está ausente: avaliações de impacto sobre a proteção de dados, encarregado de dados obrigatório, multas calculadas como percentual do faturamento e um prazo legal para notificar incidentes com dados.

Mesmo assim, a UE reconheceu a Argentina como adequada em 2003 (Decisão 2003/490/CE) e confirmou isso no relatório da Comissão de 15/01/2024. A Argentina também ratificou a Convenção 108+ modernizada do Conselho da Europa. Seus clientes na UE podem, portanto, transferir dados pessoais para a Argentina sem cláusulas contratuais padrão.

Reforma no Congresso: o projeto 3397-D-2026 foi apresentado na Câmara dos Deputados em 16/07/2026. Entre outros pontos, ele prevê um prazo para notificar incidentes com dados e

multas mais altas. Até a aprovação, a Ley 25.326 continua valendo sem alterações.

Quem já trabalha hoje no padrão do RGPD terá pouco a ajustar quando a reforma vier. Para prestadores de serviço com clientes na UE, esse é de qualquer forma o caminho mais sensato, porque o contrato de tratamento de dados do art. 28 do RGPD exige esses parâmetros independentemente do direito argentino.

Cibersegurança comparada à NIS2

A Argentina não tem lei de cibersegurança. Existe uma estratégia nacional de cibersegurança e uma equipe estatal de resposta a incidentes, o CERT.ar, ligado à Dirección Nacional de Ciberseguridad. Disso não decorrem obrigações para empresas como as que a [NIS2](#) prevê na UE para energia, transporte, saúde ou serviços digitais.

Há regras obrigatórias no setor financeiro. O banco central, BCRA, exige com a Comunicación “A” 7724 padrões mínimos de TI e de segurança da informação e regula em outras Comunicaciones a resposta a incidentes cibernéticos e sua notificação. Se você fornece software ou serviços de data center a bancos argentinos, já conhece essas exigências pelos contratos deles.

Para clientes da UE, o que conta no fim é o que está no contrato. Uma software house de Córdoba que desenvolve para uma seguradora alemã recebe cláusulas derivadas do [DORA](#). Um fabricante de controladores com conexão de rede precisa cumprir os requisitos do [Cyber Resilience Act](#) se o equipamento for vendido na UE.

Prazos de notificação comparados

SITUAÇÃO	ARGENTINA	UE
Incidente com dados, aviso à autoridade	sem prazo legal na Ley 25.326	72 horas (art. 33 do RGPD)
Aviso aos titulares	sem prazo legal	sem demora indevida, se o risco for alto (art. 34 do RGPD)
Incidente cibernético significativo	sem lei geral; bancos notificam conforme as regras do BCRA	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

Como a legislação local não fixa prazo, na prática quem define o prazo é o seu cliente da UE, no contrato. Conte com 24 a 48 horas e organize seu processo para conseguir cumprir: quem decide, quem notifica e quais informações entram na primeira notificação.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	AAIP, Dirección Nacional de Protección de Datos Personales
CSIRT	CERT.ar, Dirección Nacional de Ciberseguridad
Setor financeiro	BCRA, Banco Central de la República Argentina
Acreditação	OAA, Organismo Argentino de Acreditación

Certificados [ISO 27001](#) ou [ISO 9001](#) emitidos por organismos acreditados pelo OAA costumam ser aceitos na UE. Alguns grupos empresariais fazem questão de um certificador que já conhecem. Esclareça isso antes da auditoria.

O que os clientes da UE costumam exigir

Para o EUDR, exportadores do agronegócio precisam dos dados de geolocalização de todas as áreas em que foram produzidos a soja ou o gado destinados à UE, além da comprovação de que não houve desmatamento ali desde 31/12/2020. A Argentina está classificada como país de risco padrão. Fabricantes de alimentos também recebem pedidos de certificação [IFS](#), [BRCGS](#) ou [FSSC 22000](#).

Prestadores de serviços de TI recebem questionários de segurança, um contrato de tratamento de dados e, muitas vezes, o pedido de um certificado ISO 27001 ou de um relatório SOC 2. Um sistema de gestão da segurança da informação pode ser montado e documentado para a auditoria com uma plataforma de GRC como a [Sightadel](#).

Na prática, fornecedores argentinos recebem um pacote com vários documentos: o contrato de tratamento de dados, um anexo com as medidas técnicas e organizacionais, uma lista de subcontratados, um acordo de confidencialidade e um questionário de segurança que muitas vezes passa de cem perguntas. Uma parte dessas perguntas trata do que sua empresa expõe na internet. Um relatório da verificação externa, por exemplo do [veyrisk](#), responde a esse bloco com dados atuais. As cláusulas contratuais padrão não são necessárias graças à adequação. Mas se você repassa dados a prestadores fora da Argentina, por exemplo a um provedor de nuvem nos Estados Unidos, seu cliente da UE vai perguntar como essa transferência está protegida.

Um bom ponto de partida para empresas argentinas:

1. Identifique quais dos seus clientes estão na UE e quais regras da UE se aplicam a eles.
2. Leve seu programa de proteção de dados ao nível do RGPD, mesmo onde a Ley 25.326 exige menos. Isso também prepara você para a reforma.

3. Defina um prazo interno para notificar incidentes que seja mais curto do que qualquer prazo dos seus contratos.
4. Para exportações agrícolas, reúna os dados de geolocalização das suas áreas e das áreas dos seus fornecedores.
5. Avalie se um certificado ISO 27001 ou uma norma de segurança de alimentos pode poupar você de comprovações avulsas.

O [Diagnóstico UE](#) gratuito dá uma primeira visão das suas lacunas.

Acordo com a UE

O [acordo UE-Mercosul](#) foi assinado em 17/01/2026 em Assunção. A Argentina o ratificou em fevereiro de 2026. Desde 01/05/2026, a parte comercial é aplicada provisoriamente entre a UE e Argentina, Brasil, Paraguai e Uruguai. Para obter a preferência tarifária, você precisa de 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.

Vantagens tarifárias não mudam nada no direito de produtos da UE. EUDR, CBAM e RGPD continuam valendo integralmente.

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

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 →](#)

 veyrisk

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

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.

PAÍS · MERCOSUL

Brasil: o que os clientes da UE esperam

Desde janeiro de 2026, a UE reconhece o Brasil como país com nível adequado de proteção de dados. Isso facilita o fluxo de dados, mas não substitui as comprovações de segurança da informação, de desmatamento ou de emissões.

Visão geral: comércio com a UE

O Brasil é o maior parceiro comercial da UE na América do Sul. Segundo a Comissão Europeia, cerca de 42 % das exportações brasileiras para a UE em 2025 foram produtos agrícolas e 27 % combustíveis e produtos de mineração, principalmente petróleo bruto e também minério de ferro. Quem embarca soja do Paraná, café de Minas Gerais ou celulose de Mato Grosso do Sul para Roterdã ou Hamburgo esbarra primeiro em regras de cadeia de suprimentos como o [EUDR](#). Exportadores de aço e alumínio são afetados pelo [CBAM](#).

Some-se a isso uma exportação de serviços em crescimento: software houses de São Paulo, Florianópolis ou Recife desenvolvem para bancos, seguradoras e clientes industriais na Europa. Para elas, proteção de dados e segurança da informação pesam mais do que tarifas.

Proteção de dados: a LGPD comparada ao RGPD

A LGPD (Lei nº 13.709/2018) está em vigor desde setembro de 2020, e a ANPD aplica sanções desde agosto de 2021. Ela foi inspirada no [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais para cada tratamento, direitos dos titulares, encarregado, relatórios de impacto e o dever de comunicar incidentes de segurança. Quem implementa bem a LGPD já cumpre boa parte das obrigações do RGPD.

Desde janeiro de 2026 existe também uma decisão de adequação da UE (Decisão de Execução (UE) 2026/179). O reconhecimento é mútuo: com a Resolução CD/ANPD nº 32/2026, a ANPD também reconheceu a UE como adequada. Para os seus clientes na UE, isso significa que dados pessoais podem vir para o Brasil sem cláusulas contratuais padrão e sem avaliação de impacto da transferência. Ficam de fora apenas as transferências para fins de segurança pública e perseguição penal.

A adequação trata apenas da transferência de dados. Se você trata dados por conta de um cliente da UE, continua precisando de um contrato de tratamento de dados nos termos do art. 28 do RGPD e de comprovar suas medidas técnicas e organizacionais.

Duas diferenças aparecem na prática. A LGPD prevê dez bases legais, entre elas a proteção do crédito; o RGPD, seis. E o prazo para comunicar incidentes é contado em dias úteis, não em horas. Quem atende os dois regimes faz melhor em alinhar seus processos ao prazo mais curto.

Cibersegurança comparada à NIS2

Aqui ainda não existe uma lei que, como a [NIS2](#), fixe obrigações para setores inteiros. O Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber) e um comitê (CNCiber), mas não criou uma autoridade de supervisão com poder sobre as empresas. O projeto do Marco Legal da Cibersegurança (PL 4.752/2025) está no Senado. A principal questão em aberto é se a supervisão ficará com uma nova agência ou com a Anatel.

Até agora, as regras obrigatórias são setoriais. Pela Resolução CMN nº 4.893/2021, bancos precisam ter uma política de segurança cibernética, controlar a contratação de serviços em nuvem e comunicar incidentes relevantes ao Banco Central. Para instituições de pagamento vale algo equivalente pela Resolução BCB nº 85/2021.

Para fornecedores de clientes europeus, isso é secundário. Pela NIS2, seu cliente na UE precisa gerenciar a segurança da cadeia de suprimentos e repassa essa obrigação a você por contrato. Quem fornece software para empresas financeiras na UE recebe ainda cláusulas do [DORA](#) no contrato, e fabricantes de produtos conectados se enquadram no [Cyber Resilience Act](#).

Prazos de notificação comparados

SITUAÇÃO	BRASIL	UE
Incidente com dados, comunicação à autoridade	3 dias úteis a partir do conhecimento, se houver risco relevante (Res. CD/ANPD 15/2024); prazo em dobro para agentes de pequeno porte	72 horas (art. 33 do RGPD)
Comunicação aos titulares	também 3 dias úteis	sem demora indevida, se o risco for alto (art. 34 do RGPD)
Incidente cibernético significativo	sem lei geral; bancos comunicam ao Banco Central	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

A regra da ANPD também exige que você registre os incidentes e guarde essa documentação por cinco anos. Um cliente da UE normalmente fixa no contrato um prazo próprio, muitas vezes de 24 a 48 horas, para conseguir cumprir as 72 horas dele.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	ANPD, Autoridade Nacional de Proteção de Dados
Cibersegurança federal	GSI/PR com o CTIR Gov (administração pública federal)
CSIRT para empresas	CERT.br, do NIC.br
Setor financeiro	Banco Central do Brasil, Conselho Monetário Nacional
Acreditação	INMETRO, acreditação pela Cgcre

Certificados de organismos acreditados pela Cgcre costumam ser aceitos na UE, porque a Cgcre participa dos acordos internacionais de reconhecimento entre acreditadores. Mesmo assim, pergunte antes da auditoria se o seu cliente exige um certificador específico.

O que os clientes da UE costumam exigir

Para exportadores do agronegócio e de commodities, o EUDR vem em primeiro lugar. Seu comprador precisa dos dados de geolocalização das suas áreas e da comprovação de que não houve desmatamento ali depois de 31/12/2020. No EUDR, o Brasil está classificado como país de risco padrão. Por isso vale a diligência devida completa; a diligência devida simplificada do art. 13 só existe para países de baixo risco. Na cadeia de alimentos, somam-se certificações [IFS](#), [BRCGS](#) ou [FSSC 22000](#).

Prestadores de serviços de software e TI geralmente recebem um questionário de segurança baseado na NIS2 e na [ISO 27001](#). Perguntas típicas: em quanto tempo você comunica um incidente? Quem tem acesso aos dados de produção? Há testes de intrusão? Um certificado ISO 27001 responde a muitas dessas perguntas de uma vez. Para montar o sistema de gestão até a auditoria, a plataforma [Sightadel](#) conduz pelos requisitos da norma e guarda as comprovações.

Muitos clientes também verificam de fora o que você expõe na internet: portas abertas, certificados vencidos, versões antigas de servidor. Quem acompanha isso continuamente, por exemplo com o [veyrisk](#), já sabe a resposta antes de o questionário chegar.

No contrato, essas exigências costumam virar anexos: um contrato de tratamento de dados nos termos do art. 28 do RGPD, uma lista das medidas técnicas e organizacionais, prazos de notificação de incidentes, direitos de auditoria do cliente e regras para subcontratados. Como o Brasil é considerado adequado, as cláusulas contratuais padrão deixam de ser necessárias. O restante seu cliente exige mesmo assim, e vai revisar de novo na renovação.

Um bom ponto de partida para empresas brasileiras:

1. Verifique quais regras da UE afetam seus clientes e pergunte ativamente pelas exigências, em vez de esperar o questionário.
2. Coloque sua documentação da LGPD lado a lado com os requisitos do RGPD. Registro das operações de tratamento, bases legais e relatórios de impacto geralmente podem ser aproveitados.
3. Estruture um processo de notificação que cumpra o prazo contratual mais curto e teste esse processo uma vez por ano.
4. Para o EUDR, reúna dados de geolocalização e comprovações dos seus fornecedores antes que o comprador peça.
5. Decida se um certificado ISO 27001 ou uma norma de segurança de alimentos responde aos questionários dos clientes mais rápido do que cada informação avulsa.

O [Diagnóstico UE](#) gratuito mostra onde sua empresa está hoje.

Acordo com a UE

O [acordo UE-Mercosul](#) foi assinado em 17/01/2026 em Assunção. Sua parte comercial, o acordo comercial interino, é aplicada provisoriamente desde 01/05/2026 entre a UE e Brasil, Argentina, Paraguai e Uruguai. As tarifas caem de forma escalonada, e você precisa de uma declaração de origem para usar a preferência. 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.

O acordo não dispensa o direito da UE. EUDR, CBAM, RGPD e regulamentos de produto valem para mercadorias brasileiras da mesma forma que para mercadorias de qualquer outro país.

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

PAÍS · MERCOSUL

Paraguai: o que os clientes da UE esperam

Desde novembro de 2025, o Paraguai tem uma lei geral de proteção de dados, que passa a ser plenamente aplicável no fim de novembro de 2027, após um período de transição. Uma lei de cibersegurança ainda não existe.

Visão geral: comércio com a UE

As importações da UE vindas do Paraguai são quase só produtos agrícolas: segundo a Comissão Europeia, 82 % em 2025. Soja do leste do país e carne bovina do Chaco são os exemplos mais conhecidos. Ambas se enquadram no [EUDR](#), e é por aí que começam as perguntas dos compradores europeus.

Para o Paraguai, o acordo UE-Mercosul é o maior passo de política comercial em anos. Assunção foi o local da assinatura, em 17/01/2026.

Proteção de dados: a Ley 7593/2025 comparada ao RGPD

Até 2025, o Paraguai não tinha uma lei geral de proteção de dados; havia regras sobretudo para dados de crédito (Ley 6534/2020). A Ley Nº 7593/2025 de Protección de Datos Personales foi promulgada em 27/11/2025. Ela prevê um período de transição de 24 meses e, com isso, passa a ser plenamente aplicável no fim de novembro de 2027. O regulamento ainda não foi editado.

A lei adota muitas das ideias centrais do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais, direitos dos titulares, obrigações para controladores e operadores, regras para transferências ao exterior. A supervisão ficará com uma Agencia Nacional de Protección de Datos Personales, vinculada ao Ministério de Tecnologías da Informação e Comunicación (MITIC), com autonomia funcional. As multas vão de 20 a 10.000 diárias de salário mínimo.

O Paraguai não tem decisão de adequação da UE. Seus clientes na UE precisam, para cada transferência de dados pessoais ao Paraguai, de cláusulas contratuais padrão (Decisão de Execução (UE) 2021/914) e de uma avaliação de impacto da transferência. Isso vale também para casos simples, por exemplo quando sua equipe comercial em Assunção consulta dados de clientes no CRM de um distribuidor alemão.

Você não precisa esperar até 2027. Quem cria agora um registro das operações de tratamento, controla os acessos e monta um processo para comunicar incidentes com dados atende às

expectativas dos clientes da UE e fica preparado para a nova lei.

Cibersegurança comparada à NIS2

O Paraguai não tem lei de cibersegurança. Vários projetos tramitam no Congresso, entre eles uma “Ley de Ciberseguridad de la República del Paraguay”, apresentada em junho de 2025. Por enquanto, a base é a Estrategia Nacional de Ciberseguridad 2025 a 2028 (Decreto Nº 3900/2025). A equipe nacional de resposta a incidentes, o CERT-PY, faz parte da Dirección General de Ciberseguridad do MITIC.

Obrigações como as da [NIS2](#), ou seja, gestão de riscos, segurança da cadeia de suprimentos e prazos fixos de notificação para setores inteiros, não decorrem disso para as empresas. Para bancos, o banco central tem regras próprias de segurança da informação.

Para fornecedores do Paraguai, isso significa que as exigências chegam pelo contrato com o cliente da UE. Uma trading agrícola com software logístico próprio recebe perguntas sobre controle de acesso, backups e planos de contingência; um fabricante de equipamentos conectados, sobre o [Cyber Resilience Act](#).

Prazos de notificação comparados

SITUAÇÃO	PARAGUAI	UE
Incidente com dados, aviso à autoridade	hoje sem prazo vigente; Ley 7593/2025 a partir do fim de 11/2027, detalhes por regulamento	72 horas (art. 33 do RGPD)
Aviso aos titulares	hoje sem prazo vigente	sem demora indevida, se o risco for alto (art. 34 do RGPD)
Incidente cibernético significativo	sem lei	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

Na prática, o cliente da UE fixa o prazo no contrato, geralmente de 24 a 48 horas. Defina com antecedência quem notifica na sua empresa e quem fica de plantão caso algo aconteça no fim de semana.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO

Proteção de dados	Agencia Nacional de Protección de Datos Personales (MITIC, em estruturação)
Cibersegurança, CSIRT	MITIC, Dirección General de Ciberseguridad com o CERT-PY
Setor financeiro	BCP, Banco Central del Paraguay
Acreditação	ONA, Organismo Nacional de Acreditación (no CONACYT)

Para certificados, importa menos onde está o organismo certificador e mais quem o acreditou. Pergunte antes da contratação se a acreditação pelo ONA 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

Para exportadores de soja e carne, o EUDR vem em primeiro lugar: dados de geolocalização de todas as áreas, comprovação de origem livre de desmatamento após 31/12/2020 e comprovação de produção legal segundo o direito paraguaio. No EUDR, o Paraguai está classificado como país de risco padrão. Justamente no Chaco, onde muita floresta foi derrubada nas últimas décadas, os compradores perguntam com detalhe.

Fabricantes de alimentos geralmente precisam de uma certificação [IFS](#), [BRCGS](#) ou [FSSC 22000](#), indústrias muitas vezes de [ISO 9001](#). Quem trata dados de clientes europeus recebe cláusulas contratuais padrão e um questionário de segurança. Muitos desses questionários perguntam por sistemas acessíveis pela internet; o [veyrisk](#) verifica essa superfície de ataque de fora e entrega um relatório.

No contrato, essas exigências costumam aparecer em vários anexos: cláusulas contratuais padrão, contrato de tratamento de dados, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Além disso, seu cliente da UE precisa elaborar uma avaliação de impacto da transferência para o Paraguai. Para isso, ele precisa de informações suas sobre acessos, criptografia e possíveis solicitações de autoridades. Quanto mais precisas forem suas respostas, mais rápido o contrato é assinado.

Um bom ponto de partida para empresas do Paraguai:

1. Identifique quais dados você recebe de clientes da UE e onde eles ficam armazenados.
2. Crie um registro das operações de tratamento e nomeie uma pessoa responsável pela proteção de dados. Você vai precisar das duas coisas, no máximo, com a Ley 7593/2025.

3. Monte um processo de notificação de incidentes que cumpra os prazos dos seus contratos.
4. Para exportações de soja e carne, reúna os dados de geolocalização das suas áreas e das áreas dos seus fornecedores.
5. Veja qual certificado seus clientes pedem com mais frequência e planeje a auditoria com antecedência.

O [Diagnóstico UE](#) gratuito mostra onde sua empresa está hoje.

Acordo com a UE

O [acordo UE-Mercosul](#) foi assinado em 17/01/2026 em Assunção. Desde 01/05/2026, a parte comercial é aplicada provisoriamente entre a UE e Paraguai, Argentina, Brasil e Uruguai. Para obter a preferência tarifária, você precisa de 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.

O acordo reduz tarifas, não exigências. EUDR, CBAM e RGPD valem integralmente para mercadorias paraguaias.

<https://www.mercoeu.com/pt/paises/paraguai>

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.

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

ÁREA	ÓRGÃO
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 Montevideu 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.

<https://www.mercoeu.com/pt/paises/uruguai>

PAÍS · MERCOSUL

Bolívia: o que os clientes da UE esperam

A Bolívia é membro pleno do Mercosul desde 2024, mas ainda está incorporando suas regras aos poucos. Não existe lei de proteção de dados nem lei de cibersegurança. Clientes da UE preenchem essa lacuna com contratos.

Visão geral: comércio com a UE

A Bolívia fornece à Europa principalmente matérias-primas e produtos agrícolas, como minérios do Altiplano, castanha-do-pará da região amazônica em torno de Riberalta e quinoa. A Comissão não publica um detalhamento só para a Bolívia. Para os países andinos em conjunto, ela aponta para 2025 produtos agrícolas, produtos minerais e pesca como os maiores grupos.

A Bolívia não tem acordo comercial com a UE. As vantagens tarifárias vêm do Sistema de Preferências Generalizadas da UE, incluindo o regime especial SPG+ de incentivo ao desenvolvimento sustentável e à boa governança. Essas preferências dependem do cumprimento de convenções internacionais sobre direitos humanos, trabalho e meio ambiente.

Proteção de dados comparada ao RGPD

A Bolívia não tem lei geral de proteção de dados. A privacidade é protegida pela Constituição, que prevê uma ação própria para sua defesa (Acción de Protección de Privacidad, comparável ao habeas data de outros países), e pelo direito processual constitucional. Projetos de lei de proteção de dados foram discutidos, mas nenhum foi promulgado. Por isso não existe autoridade de proteção de dados nem obrigação legal de notificar incidentes com dados.

O [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#) independe disso. Ele se aplica diretamente à sua empresa se você oferece produtos ou serviços de forma direcionada a pessoas na UE. E se aplica pelo contrato quando você trata dados por conta de um cliente da UE.

Não existe decisão de adequação da UE. Para cada transferência de dados pessoais à Bolívia, seu cliente da UE precisa de cláusulas contratuais padrão (Decisão de Execução (UE) 2021/914) e de uma avaliação de impacto da transferência. Nessa avaliação, ele verifica se o direito boliviano compromete a proteção dos dados. Como falta uma lei de proteção de dados, ele vai exigir medidas técnicas adicionais, como criptografia e regras rígidas de acesso.

Sem uma legislação local como referência, suas próprias regras são a comprovação. Uma política de proteção de dados por escrito, um registro das operações de tratamento e um processo de notificação já testado pesam mais na avaliação de impacto da transferência do que qualquer promessa.

Cibersegurança comparada à NIS2

A Bolívia não tem lei de cibersegurança. As regras de segurança da informação valem sobretudo para a administração pública. A equipe de resposta a incidentes, o CGII (Centro de Gestión de Incidentes Informáticos), faz parte da agência estatal de governo eletrônico e TIC, a AGETIC. No setor financeiro, o órgão supervisor ASFI tem exigências próprias de segurança da informação.

Isso não é comparável à [NIS2](#). Na UE, a NIS2 obriga empresas médias e grandes de 18 setores a fazer gestão de riscos, cuidar da segurança da cadeia de suprimentos e cumprir prazos fixos de notificação. Seus clientes na UE precisam cumprir essas obrigações e as repassam por contrato aos fornecedores, ou seja, também a você.

Quem vende para a UE equipamentos com software ou conexão de rede também se enquadra no [Cyber Resilience Act](#).

Prazos de notificação comparados

SITUAÇÃO	BOLÍVIA	UE
Incidente com dados, aviso à autoridade	sem obrigação, sem autoridade	72 horas (art. 33 do RGPD)
Aviso aos titulares	sem obrigação	sem demora indevida, se o risco for alto (art. 34 do RGPD)
Incidente cibernético significativo	sem lei; regras para a administração pública e o setor financeiro	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

Como a legislação local não define nada, vale o prazo do seu contrato. Clientes da UE costumam exigir a notificação em 24 a 48 horas. Defina quem notifica e quais informações a primeira notificação deve conter.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO

Proteção de dados	nenhuma autoridade
Cibersegurança, CSIRT	AGETIC com o CGII
Setor financeiro	ASFI, Autoridad de Supervisión del Sistema Financiero
Acreditação	DTA, Dirección Técnica de Acreditación do IBMETRO

O que os clientes da UE costumam exigir

Onde a lei é omissa, contam certificados e comprovações. Um exportador de castanha-do-pará precisa de certificações de alimentos [IFS](#), [BRCGS](#) ou [FSSC 22000](#) e de rastreabilidade completa. Mineradoras recebem perguntas sobre padrões ambientais e trabalhistas, muitas vezes com referência à [ISO 14001](#) e aos deveres europeus de diligência na cadeia de suprimentos. Gado, soja e madeira das terras baixas se enquadram no [EUDR](#).

Prestadores que tratam dados para clientes da UE recebem cláusulas contratuais padrão, um questionário de segurança e, com frequência, a pergunta sobre a [ISO 27001](#). Uma plataforma de GRC como a [Sightadel](#) ajuda a manter políticas, riscos e comprovações em um só lugar quando nenhuma lei dá a estrutura.

Na avaliação de impacto da transferência, seu cliente da UE precisa descrever quem na Bolívia poderia acessar os dados e como ele os protege. Para isso, ele pergunta a você sobre locais de armazenamento, criptografia, direitos de acesso, registros e o tratamento de pedidos de informação de autoridades. Tenha essas informações por escrito. Um documento que você possa entregar a vários clientes economiza semanas de alinhamento.

Um bom ponto de partida para empresas bolivianas:

1. Identifique quais dos seus clientes estão na UE e quais regras da UE valem para as compras deles.
2. Escreva uma política própria de proteção de dados no modelo do RGPD, com registro das operações de tratamento e regras de exclusão.
3. Defina um prazo de notificação de incidentes e quem é responsável por notificar.
4. Para exportações agrícolas e de madeira, verifique se o EUDR se aplica e reúna os dados de geolocalização.
5. Escolha o certificado que seus clientes pedem com mais frequência e planeje a auditoria com um organismo reconhecido.

O [Diagnóstico UE](#) gratuito mostra suas lacunas.

Acordo com a UE

A Bolívia é Estado Parte do Mercosul desde 2024. Ela depositou o instrumento de ratificação do Protocolo de Adesão em 08/07/2024, em Assunção (Ley 1567, de 04/07/2024), e a adesão entrou em vigor 30 dias depois. Para incorporar o direito do Mercosul e a Tarifa Externa Comum, tem um período de transição de até quatro anos. A Bolívia não participa do [acordo UE-Mercosul](#), aplicado provisoriamente desde 01/05/2026 com Argentina, Brasil, Paraguai e Uruguai. As vantagens tarifárias desse acordo, portanto, não valem para mercadorias bolivianas.

A Comissão observa que a Bolívia poderia aderir ao acordo comercial com Colômbia, Peru e Equador. Até lá, o SPG+ continua sendo o caminho para o mercado da UE.

Na prática, isso significa: verifique para cada mercadoria a alíquota e a regra de origem no portal Access2Markets da Comissão Europeia, organizado por código de mercadoria. Para usar a preferência do SPG, os exportadores geralmente precisam estar inscritos no sistema eletrônico de exportadores registrados da Comissão (REX) e fazer uma declaração de origem na fatura. Seu importador na UE costuma conhecer o procedimento e pode ajudar. Guarde as comprovações por vários anos, porque a alfândega pode verificar depois. Como o SPG+ depende de condições, vale acompanhar os relatórios da Comissão sobre o cumprimento por parte da Bolívia.

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

PAÍS · ASSOCIADO AO MERCOSUL

Chile: o que os clientes da UE esperam

O Chile tem a lei de cibersegurança mais próxima da NIS2 na região e uma nova lei de proteção de dados que deve entrar em vigor em 01/12/2026. Desde fevereiro de 2025, o país está ligado à UE por um acordo comercial modernizado.

Visão geral: comércio com a UE

Segundo a Comissão Europeia, as importações da UE vindas do Chile em 2025 foram compostas em 40% por produtos vegetais, em 20% por produtos minerais e em 20% por metais comuns. Por trás desses números estão frutas e vinhos do Vale Central, o cobre de Antofagasta e o lítio do Atacama. O cobre, aliás, não está no [CBAM](#). Aço, alumínio e fertilizantes estão.

Santiago também é um polo importante de prestadores de serviços de TI, data centers e fintechs que atendem clientes na Espanha e em outros países da UE.

Proteção de dados: Ley 21.719 e o RGPD

A Ley 21.719 reforma a fundo a antiga lei de proteção de dados, a Ley 19.628. Ela foi publicada no Diário Oficial em 13/12/2024 e entra em vigor em 01/12/2026. A lei adota muitos elementos do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais, direitos ampliados dos titulares, incluindo a portabilidade, obrigações para operadores, regras para transferências ao exterior e o dever de notificar incidentes de segurança. A novidade é uma autoridade de controle própria, a Agencia de Protección de Datos Personales, com poder para aplicar multas.

Possível adiamento: em 31/08/2026 o governo apresentou o projeto de lei Boletín 18.623-07. Ele adiaría a entrada em vigor para 01/12/2027 e ampliaria o conselho da agência. Em 11/10/2026 o projeto ainda não tinha sido aprovado, portanto continua valendo a data de 01/12/2026.

O Chile não tem decisão de adequação da UE. Seus clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência para enviar dados ao Chile.

Cibersegurança comparada à NIS2

A Ley 21.663, Ley Marco de Ciberseguridad, foi publicada em abril de 2024. A agência nacional de cibersegurança, a ANCI, funciona desde 01/01/2025, e as demais disposições valem desde 01/03/2025. Assim como a [NIS2](#), a lei distingue dois grupos: prestadores de serviços essenciais e

operadores de importância vital (Operadores de Importancia Vital, OIV). Ambos precisam notificar ao CSIRT Nacional os incidentes com impacto significativo. Os OIV têm ainda obrigações sobre sistemas de gestão, planos de contingência e auditorias.

Nos prazos, o Chile é mais rígido que a UE. O alerta precoce tem de chegar em até três horas, enquanto a NIS2 pede 24 horas. Os detalhes estão no Regulamento de Reporte de Incidentes (Decreto 295/2024).

No setor financeiro valem também as normas da comissão do mercado financeiro, a CMF, sobre segurança da informação, cibersegurança e notificação de incidentes operacionais. Quem fornece para bancos ou seguradoras europeus recebe, além disso, cláusulas da [DORA](#).

Prazos de notificação comparados

SITUAÇÃO	CHILE	UE
Alerta precoce de incidente cibernético	3 horas a partir do conhecimento (Ley 21.663)	24 horas (art. 23 da NIS2)
Atualização	72 horas; OIV com serviço essencial afetado, 24 horas	72 horas
Relatório final	15 dias corridos a partir do alerta precoce	um mês
Plano de ação dos OIV	no máximo 7 dias corridos	sem equivalente
Violação de dados à autoridade	dever de notificação pela Ley 21.719 a partir da entrada em vigor	72 horas (art. 33 do RGPD)

Quem cumpre os prazos chilenos também cumpre os da NIS2. Um processo de notificação pensado para três horas não precisa de uma segunda versão para clientes da UE.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	Agencia de Protección de Datos Personales (nova, criada pela Ley 21.719)
Cibersegurança	ANCI, Agencia Nacional de Ciberseguridad
CSIRT	CSIRT Nacional, vinculado à ANCI
Setor financeiro	CMF, Comisión para el Mercado Financiero

ÁREA	ÓRGÃO
Acreditação	INN, Instituto Nacional de Normalización

Para certificados, o que conta é menos onde fica o organismo certificador e mais quem o acreditou. Antes de contratar, pergunte se a acreditação pelo INN ou por um organismo 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 ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

O que os clientes da UE costumam exigir

Exportadores de frutas e vinhos são questionados sobre segurança de alimentos, em geral com certificados [IFS](#), [BRCGS](#) ou [FSSC 22000](#) ou GLOBALG.A.P. Madeira e celulose entram na [EUDR](#). Lá o Chile está classificado como país de baixo risco, então a diligência devida é simplificada, mas não dispensável. Mineradoras recebem perguntas sobre meio ambiente, direitos humanos e emissões, muitas vezes com referência à [ISO 14001](#).

Prestadores de serviços de TI e data centers são questionados sobre a [ISO 27001](#). Quem já está sujeito à Ley 21.663 como OIV ou prestador de serviços essenciais já montou o processo de notificação e o sistema de gestão e pode usar isso como comprovação perante clientes da UE. Uma plataforma GRC como o [Sightadel](#), que traz a NIS2 e a ISO 27001 como marcos próprios, ajuda a manter essas comprovações organizadas. Muitos clientes também verificam seus sistemas acessíveis pela internet. Com o [veyrisk](#) você mesmo acompanha essa superfície de ataque.

No contrato, esses pontos costumam aparecer em anexos: cláusulas contratuais padrão, contrato de tratamento de dados como operador, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Para a avaliação de impacto da transferência, seu cliente na UE vai perguntar onde os dados ficam armazenados, quem tem acesso e como é feita a criptografia. Com a Ley 21.719 e uma autoridade de proteção de dados própria, você poderá apontar um marco legal mais próximo do europeu.

Um bom ponto de partida para empresas chilenas:

1. Verifique se sua empresa está sujeita à Ley 21.663, como prestadora de serviços essenciais ou como OIV.
2. Prepare-se para a Ley 21.719 como se a data de 01/12/2026 fosse certa. O que você fizer para isso, seus clientes na UE já esperam de qualquer forma.

3. Reúna em um único fluxo as notificações para a ANCI, para a nova agência de proteção de dados e para seus clientes na UE.
4. Para madeira, celulose e outros produtos da EUDR, verifique com seu comprador a diligência devida simplificada.
5. Para aço, alumínio e fertilizantes, esclareça quais dados de emissões seu importador precisa para o CBAM.

Uma visão rápida da sua situação está no [Diagnóstico UE](#) gratuito.

Acordo com a UE

O Chile é associado ao Mercosul, mas não faz parte do Acordo UE-Mercosul. Tem um conjunto próprio de tratados com a UE: o Advanced Framework Agreement e o Acordo Comercial Provisório, ambos assinados em 13/12/2023. O Acordo Comercial Provisório está em vigor desde 01/02/2025 e substitui a parte comercial do Acordo de Associação de 2002. Ele traz, entre outros, capítulos sobre energia e matérias-primas e sobre desenvolvimento sustentável. Para a preferência tarifária, você precisa de uma declaração de origem.

Na prática, isso significa: confira para cada produto a tarifa e a regra de origem no portal Access2Markets da Comissão Europeia, organizado por código de mercadoria. A maior parte do comércio entre o Chile e a UE é isenta de tarifas. Para produtos processados, a regra de origem define se houve agregação de valor suficiente no Chile. Para lítio e cobre, o acordo tem regras próprias sobre matérias-primas e energia. Seu importador na UE pode ajudar a emitir a declaração de origem corretamente. Guarde os comprovantes por vários anos, porque a alfândega pode fazer verificações posteriores.

Mesmo com o acordo, EUDR, CBAM e RGPD continuam valendo da mesma forma para produtos e serviços chilenos.

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

PAÍS · ASSOCIADO AO MERCOSUL

Colômbia: o que os clientes da UE esperam

A Colômbia tem uma legislação de proteção de dados consolidada, com fiscalização ativa, mas não tem lei de cibersegurança. Com a UE, há um acordo comercial desde 2013.

Visão geral: comércio com a UE

A Colômbia fornece à UE sobretudo matérias-primas e produtos agrícolas, entre eles café de Huila e do Eixo Cafeeiro, bananas de Urabá, flores de corte da Sabana de Bogotá, abacates e carvão. A página da Comissão sobre o país não traz uma divisão só para a Colômbia. Para os países andinos em conjunto, ela indica para 2025 produtos agrícolas (48,7%), produtos minerais (27,1%) e pesca (13,5%).

Ao lado disso, cresce a exportação de serviços de TI. Equipes em Medellín, Bogotá e Cali desenvolvem software e prestam suporte a clientes na Espanha e em outros países da UE.

Proteção de dados: Ley 1581 e o RGPD

A base é a Ley Estatutaria 1581 de 2012 com seus decretos regulamentadores (Decreto 1377/2013 e Decreto 886/2014, hoje consolidados no Decreto Único 1074/2015). A autoridade de controle é a SIC (Superintendencia de Industria y Comercio), que tem uma área própria para proteção de dados. A SIC faz fiscalizações e aplica multas.

O direito colombiano se apoia mais no consentimento do que o [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#), que reconhece várias bases legais de mesmo peso. Empresas a partir de determinado porte precisam inscrever suas bases de dados no Registro Nacional de Bases de Datos (RNBD). É também ali que se notificam as violações de dados. Os controladores devem ter políticas escritas de tratamento de dados, o que na prática se aproxima de um programa de proteção de dados nos moldes do RGPD.

A Colômbia não tem decisão de adequação da UE. Seus clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência. No sentido inverso, a SIC também controla as transferências da Colômbia para o exterior. Quem movimenta dados nas duas direções precisa observar os dois regimes.

Cibersegurança comparada à NIS2

A Colômbia não tem lei de cibersegurança. A base é o documento de política CONPES 3995 de 2020, sobre confiança e segurança digital, e o Decreto 338 de 2022, que regula a governança da segurança digital. Uma agência nacional de segurança digital é discutida há anos, mas não foi criada. A equipe estatal de resposta a emergências é o ColCERT, vinculado ao Ministério de Tecnologias da Informação e Comunicações (MinTIC).

Em comparação com a [NIS2](#), faltam obrigações intersetoriais de gestão de riscos e prazos de notificação. O setor financeiro é mais regulado: a Superintendencia Financiera exige de bancos e outras entidades supervisionadas medidas de cibersegurança e a notificação de incidentes (Circular Externa 007 de 2018, hoje parte da Circular Básica Jurídica).

Para fornecedores de clientes europeus, as obrigações vêm do contrato: cláusulas da NIS2 sobre a cadeia de suprimentos, a [DORA](#) no caso de clientes financeiros e o [Cyber Resilience Act](#) no caso de produtos conectados.

Prazos de notificação comparados

SITUAÇÃO	COLÔMBIA	UE
Violação de dados à autoridade	15 dias úteis a partir do conhecimento, pelo RNBD à SIC	72 horas (art. 33 do RGPD)
Incidente cibernético significativo	sem lei geral; setor financeiro conforme as normas da Superintendencia Financiera	24 h para o alerta precoce, 72 h para a notificação, relatório final após um mês (art. 23 da NIS2)

O prazo colombiano é bem mais longo que o europeu. Se você trata dados para um cliente da UE, vale o prazo do contrato, em geral de 24 a 48 horas, para que o cliente consiga cumprir as 72 horas dele.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	SIC, Superintendencia de Industria y Comercio
Cibersegurança, CSIRT	MinTIC com o ColCERT
Setor financeiro	Superintendencia Financiera de Colombia
Acreditação	ONAC, Organismo Nacional de Acreditación de Colombia

Para certificados, o que conta é menos onde fica o organismo certificador e mais quem o acreditou. Antes de contratar, pergunte se a acreditação pelo ONAC ou por um organismo 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 ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

O que os clientes da UE costumam exigir

Exportadores de café, cacau e óleo de palma precisam cumprir a [EUDR](#): geolocalização das fincas, comprovação de produção livre de desmatamento após 31/12/2020 e comprovação de produção legal. A Colômbia está classificada como país de risco padrão. Para uma cooperativa em Huila com centenas de pequenas propriedades, reunir os polígonos é o maior trabalho. Exportadores de banana e flores são questionados sobre certificados como GLOBALG.A.P. ou sobre [normas de segurança de alimentos](#).

Prestadores de serviços de TI recebem cláusulas contratuais padrão, um questionário de segurança e muitas vezes a pergunta sobre a [ISO 27001](#). Quem quer montar um sistema de gestão de segurança da informação pode manter políticas, riscos e evidências em uma plataforma de GRC como o [Sightadel](#).

No contrato, esses pontos costumam aparecer como anexos: cláusulas contratuais padrão, contrato de tratamento de dados como operador, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Para a avaliação de impacto da transferência, seu cliente na UE vai perguntar onde os dados ficam armazenados, quem tem acesso e como é feita a criptografia. Como na Colômbia você já mantém políticas de tratamento de dados e registra bases no RNBD, parte das respostas já está documentada.

Um bom ponto de partida para empresas colombianas:

1. Identifique quais dos seus clientes estão na UE e quais regras valem para eles.
2. Compare suas políticas segundo a Ley 1581 com os requisitos do RGPD, sobretudo em bases legais e prazos de eliminação.
3. Reduza seu prazo interno de notificação de incidentes para bem abaixo dos 15 dias úteis da SIC.
4. Para café, cacau e óleo de palma, reúna a geolocalização de todas as áreas, inclusive as dos seus fornecedores.
5. Avalie se um certificado ISO 27001 ou uma norma de segurança de alimentos responde a muitas perguntas isoladas de uma só vez.

Para ver onde você está hoje, faça o [Diagnóstico UE](#) gratuito.

Acordo com a UE

A Colômbia é associada ao Mercosul, mas não faz parte do Acordo UE-Mercosul. Com a UE vale o Acordo Comercial com a Colômbia, o Peru e o Equador, aplicado provisoriamente com a Colômbia desde 01/08/2013. Para a preferência tarifária, você precisa de uma prova de origem. O acordo tem um capítulo sobre comércio e desenvolvimento sustentável, com referências às normas fundamentais do trabalho da OIT e a acordos ambientais internacionais.

Na prática, isso significa: confira para cada produto a tarifa e a regra de origem no portal Access2Markets da Comissão Europeia, organizado por código de mercadoria. Muitos produtos agrícolas e industriais estão isentos de tarifas há anos, e para alguns valem cotas ou regras de transição. Para produtos processados, a regra de origem define se houve agregação de valor suficiente no país. Seu importador na UE pode ajudar a emitir a prova de origem corretamente. Guarde a documentação por vários anos, porque a alfândega pode fazer verificações posteriores.

Normas da UE como EUDR, CBAM e RGPD valem para produtos e serviços colombianos independentemente do acordo.

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

PAÍS · ASSOCIADO AO MERCOSUL

Peru: o que os clientes da UE esperam

O Peru modernizou sua legislação de proteção de dados em 2025 e exige a notificação de violações de dados em até 48 horas. Desde o fim de 2025, serviços digitais em setores importantes também têm de notificar incidentes ao centro nacional de segurança digital.

Visão geral: comércio com a UE

O Peru exporta para a UE principalmente produtos da mineração e do agro: concentrados de cobre e zinco dos Andes, mirtilos, abacates e uvas do litoral, café de Cajamarca e Junín, além de farinha de peixe. A Comissão publica os números apenas para os países andinos em conjunto. Em 2025, 48,7% corresponderam a produtos agrícolas, 27,1% a produtos minerais e 13,5% à pesca.

Para exportadores de café e cacau, a [EUDR](#) é a maior obrigação nova. Mineradoras recebem perguntas sobretudo sobre meio ambiente, condições de trabalho e emissões.

Proteção de dados: Ley 29733 e o RGPD

A base é a Ley Nº 29733, de 2011, sobre proteção de dados pessoais. O novo regulamento, o Decreto Supremo Nº 016-2024-JUS, está em vigor desde 30/03/2025 e substitui o regulamento anterior, de 2013. Ele aproxima bastante o direito peruano do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): encarregados de proteção de dados para determinados controladores, obrigações nas transferências internacionais, regras para operadores e, principalmente, um prazo fixo para notificar violações de dados. A autoridade de controle é a Autoridad Nacional de Protección de Datos Personales (ANPD), ligada ao Ministério da Justiça. Atenção para não confundir com a ANPD brasileira, que tem a mesma sigla.

Com 48 horas, o prazo de notificação é mais curto que as 72 horas do RGPD. Especialistas interpretam de formas diferentes quando exatamente a notificação passa a ser devida. Na dúvida, notifique. Um prestador de serviços peruano que trata dados para um cliente da UE precisa, portanto, ser rápido tanto com o cliente quanto com a ANPD.

O Peru não tem decisão de adequação da UE. Os clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência.

Cibersegurança comparada à NIS2

Com a Ley Nº 30999 (Ley de Ciberdefensa), de 2019, o Peru tem uma lei de ciberdefesa do Estado. Ela trata das funções das Forças Armadas e do Estado, não de obrigações para empresas. Uma lei de cibersegurança que, como a NIS2, imponha deveres às empresas não existe. No Congresso há apenas projetos. A base é o Marco de Confianza Digital (Decreto de Urgencia Nº 007-2020), junto com a lei de governo digital (Decreto Legislativo 1412). O regulamento correspondente, o Decreto Supremo Nº 126-2025-PCM, foi publicado em novembro de 2025. Por ele, prestadores de serviços digitais em setores como finanças, serviços básicos, saúde, transporte, acesso à internet e educação devem notificar incidentes críticos ao Centro Nacional de Seguridad Digital (CNSD).

A abordagem lembra a da [NIS2](#): obrigações para setores importantes, um ponto central de notificação e prazos curtos. A NIS2 vai além, por exemplo nas obrigações de gestão de riscos, na cadeia de suprimentos e na responsabilidade pessoal da alta direção. Bancos e seguradoras têm ainda normas próprias do órgão supervisor SBS sobre segurança da informação e cibersegurança.

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

Prazos de notificação comparados

SITUAÇÃO	PERU	UE
Violação de dados à autoridade	48 horas a partir do conhecimento, à ANPD (DS 016-2024-JUS)	72 horas (art. 33 do RGPD)
Incidente crítico em serviços digitais	48 horas, ao CNSD (DS 126-2025-PCM)	24 h para o alerta precoce, 72 h para a notificação, relatório final após um mês (art. 23 da NIS2)

Um incidente com dados pessoais pode gerar as duas notificações, à ANPD e ao CNSD. Preveja isso no seu processo, com um responsável definido para cada notificação.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	ANPD, Ministerio de Justicia y Derechos Humanos
Segurança digital	Secretaría de Gobierno y Transformación Digital (PCM)

ÁREA	ÓRGÃO
CSIRT	Centro Nacional de Seguridad Digital com o PeCERT
Setor financeiro	SBS, Superintendencia de Banca, Seguros y AFP
Acreditação	INACAL, Instituto Nacional de Calidad

Para certificados, o que conta é menos onde fica o organismo certificador e mais quem o acreditou. Antes de contratar, pergunte se a acreditação pelo INACAL ou por um organismo 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 ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

O que os clientes da UE costumam exigir

Um exportador de café de Junín precisa, para a EUDR, da geolocalização de todas as parcelas dos seus fornecedores e da comprovação de que não houve desmatamento ali após 31/12/2020. O Peru está classificado como país de risco padrão. Exportadores de frutas são questionados sobre [IFS](#), [BRCGS](#) ou [FSSC 22000](#) e GLOBALG.A.P., e mineradoras, com frequência, sobre a [ISO 14001](#).

Prestadores de serviços de TI e de outsourcing recebem cláusulas contratuais padrão, questionários de segurança e a pergunta sobre a [ISO 27001](#). Muitos clientes da UE também verificam quais sistemas dos seus fornecedores estão expostos na internet. Com o [veyrisk](#) você mesmo vê essa superfície de ataque antes que o cliente pergunte.

No contrato, esses pontos costumam aparecer em anexos: cláusulas contratuais padrão, contrato de tratamento de dados como operador, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Para a avaliação de impacto da transferência, seu cliente na UE vai perguntar onde os dados ficam armazenados, quem tem acesso e como é feita a criptografia. Aqui ajuda o fato de o direito peruano, com o novo regulamento, já prever um prazo curto de notificação e obrigações para operadores. As medidas técnicas e organizacionais e as comprovações para esses anexos podem ser organizadas no [Sightadel](#), que é desenvolvido e hospedado na Alemanha.

Um bom ponto de partida para empresas peruanas:

1. Verifique se sua empresa, como prestadora de serviços digitais, está sujeita ao DS 126-2025-PCM.
2. Compare sua documentação segundo o DS 016-2024-JUS com os requisitos do RGPD.
3. Monte um processo de notificação que atenda a ANPD, o CNSD e seus clientes na UE dentro do mesmo prazo.

4. Para café e cacau, reúna a geolocalização de todas as parcelas, inclusive as dos seus fornecedores.
5. Veja qual certificado seus clientes pedem com mais frequência e planeje a auditoria com um organismo reconhecido.

Uma primeira visão geral está no [Diagnóstico UE](#) gratuito.

Acordo com a UE

O Peru é associado ao Mercosul, mas não faz parte do Acordo UE-Mercosul. Com a UE vale o Acordo Comercial com a Colômbia, o Peru e o Equador, aplicado provisoriamente com o Peru desde 01/03/2013. Para a preferência tarifária, você precisa de uma prova de origem. O capítulo sobre comércio e desenvolvimento sustentável faz referência às normas fundamentais do trabalho da OIT e a acordos ambientais internacionais.

Na prática, isso significa: confira para cada produto a tarifa e a regra de origem no portal Access2Markets da Comissão Europeia, organizado por código de mercadoria. Muitos produtos agrícolas e industriais estão isentos de tarifas há anos, e para alguns valem cotas ou regras de transição. Para produtos processados, a regra de origem define se houve agregação de valor suficiente no país. Seu importador na UE pode ajudar a emitir a prova de origem corretamente. Guarde a documentação por vários anos, porque a alfândega pode fazer verificações posteriores.

EUDR, CBAM e RGPD valem para produtos e serviços peruanos independentemente do acordo.

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

PAÍS · ASSOCIADO AO MERCOSUL

Equador: o que os clientes da UE esperam

O Equador tem desde 2021 uma lei de proteção de dados inspirada no modelo europeu e, desde maio de 2026, uma lei para o fortalecimento da cibersegurança. Com a UE, o país mantém um acordo comercial desde 2017.

Visão geral: comércio com a UE

O Equador fornece à Europa sobretudo alimentos: bananas de El Oro e Los Ríos, camarão do Golfo de Guayaquil, atum em conserva de Manta, cacau e flores de corte da serra. A Comissão publica os números apenas para os países andinos em conjunto. Em 2025, 48,7% corresponderam a produtos agrícolas, 27,1% a produtos minerais e 13,5% à pesca, área em que o Equador é especialmente forte.

Para exportadores de cacau e óleo de palma vale a [EUDR](#). Empresas de pesca e de alimentos precisam ainda da habilitação da UE para alimentos de origem animal e de certificados de segurança de alimentos sólidos.

Proteção de dados: LOPDP e o RGPD

A Ley Orgánica de Protección de Datos Personales (LOPDP) foi publicada no Registro Oficial em maio de 2021. Depois de um período de transição de dois anos, as sanções também valem desde maio de 2023. O regulamento é o Decreto Ejecutivo 904, de 2023. A autoridade de controle é a Superintendencia de Protección de Datos Personales (SPDP).

A LOPDP segue de perto o [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais, direitos dos titulares, encarregados de proteção de dados, avaliações de impacto, obrigações para operadores e regras para transferências internacionais. Quem conhece o RGPD se orienta rápido.

A diferença está no prazo para notificar violações de dados: o art. 43 da LOPDP exige a notificação à SPDP em no máximo cinco dias após a violação. Os operadores devem informar o controlador em até dois dias. A notificação é feita por um sistema eletrônico da SPDP.

O Equador não tem decisão de adequação da UE. Seus clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência.

Cibersegurança comparada à NIS2

Desde 22/05/2026 está em vigor a Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada no Registro Oficial. O objetivo declarado é proteger a infraestrutura crítica e garantir a

continuidade dos serviços essenciais. A lei cria um Sistema Nacional de Ciberseguridad e altera sete leis existentes, entre elas a LOPDP e a lei de telecomunicações. O foco está nos órgãos públicos e nos operadores de infraestrutura crítica.

A abordagem se parece com a da [NIS2](#), que mira entidades essenciais e importantes em 18 setores. Se sua empresa está abrangida, quais obrigações de gestão de riscos se aplicam e em que prazo os incidentes devem ser notificados, você deve conferir no texto da lei no Registro Oficial e nas normas de regulamentação. Uma empresa que já trabalha conforme a [ISO 27001](#) provavelmente já cobre a maior parte dos requisitos.

Para fornecedores de clientes europeus, as exigências contratuais valem de qualquer forma: cláusulas da NIS2 sobre a cadeia de suprimentos, a [DORA](#) no caso de clientes financeiros e o [Cyber Resilience Act](#) no caso de produtos conectados.

Prazos de notificação comparados

SITUAÇÃO	EQUADOR	UE
Violação de dados à autoridade	no máximo 5 dias após a violação, à SPDP (art. 43 da LOPDP)	72 horas (art. 33 do RGPD)
Operador ao controlador	2 dias	sem demora injustificada (art. 33(2) do RGPD)
Incidente cibernético significativo	lei em vigor desde 22/05/2026; conferir prazo e destinatário no texto do Registro Oficial	24 h para o alerta precoce, 72 h para a notificação, relatório final após um mês (art. 23 da NIS2)

Se você trata dados para um cliente da UE, vale o prazo do contrato, em geral de 24 a 48 horas. Os dois dias que a LOPDP dá aos operadores normalmente não bastam para isso.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	SPDP, Superintendencia de Protección de Datos Personales
CSIRT	EcuCERT, vinculado à ARCOTEL
Setor financeiro	Superintendencia de Bancos
Acreditação	SAE, Servicio de Acreditación Ecuatoriano

Para certificados, o que conta é menos onde fica o organismo certificador e mais quem o acreditou. Antes de contratar, pergunte se a acreditação pelo SAE ou por um organismo 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 ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

Qual órgão recebe as notificações pela nova lei de cibersegurança, o melhor é verificar diretamente no texto da lei ou com o seu órgão regulador setorial.

O que os clientes da UE costumam exigir

Um criador de camarão de El Oro que vende para um atacadista na Espanha precisa da habilitação do seu estabelecimento para o mercado da UE, de rastreabilidade até o viveiro e, em geral, de um certificado [IFS](#), [BRCGS](#) ou [FSSC 22000](#). Exportadores de banana e flores são questionados sobre GLOBALG.A.P. Exportadores de cacau precisam entregar, para a EUDR, a geolocalização das parcelas e a comprovação de produção livre de desmatamento após 31/12/2020. O Equador está classificado como país de risco padrão.

Prestadores de serviços de TI recebem cláusulas contratuais padrão, questionários de segurança e a pergunta sobre a [ISO 27001](#). Quem monta um sistema de gestão conforme a ISO 27001 pode manter políticas, riscos e evidências em uma plataforma de GRC como o [Sightadel](#). Para as perguntas sobre os seus sistemas acessíveis pela internet, o [veyrisk](#) fornece um relatório da superfície de ataque externa que pode ser anexado ao questionário.

No contrato, esses pontos costumam aparecer em anexos: cláusulas contratuais padrão, contrato de tratamento de dados como operador, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Para a avaliação de impacto da transferência, seu cliente na UE vai perguntar onde os dados ficam armazenados, quem tem acesso e como é feita a criptografia. A LOPDP dá uma boa base para isso, porque adota muitos conceitos e obrigações do RGPD.

Um bom ponto de partida para empresas equatorianas:

1. Verifique se sua empresa está sujeita à lei de cibersegurança de 2026.
2. Compare sua documentação segundo a LOPDP com os requisitos do RGPD. As lacunas costumam ser pequenas.
3. Reduza seu prazo interno de notificação de incidentes para bem abaixo dos cinco dias da LOPDP.
4. Para cacau e óleo de palma, reúna a geolocalização de todas as parcelas, inclusive as dos seus fornecedores.

5. Mantenha atualizados as habilitações, a rastreabilidade e os certificados de segurança de alimentos para camarão, atum e banana.

Para ver onde você está hoje, faça o [Diagnóstico UE](#) gratuito.

Acordo com a UE

O Equador é associado ao Mercosul, mas não faz parte do Acordo UE-Mercosul. O país aderiu ao Acordo Comercial da UE com a Colômbia e o Peru, aplicado desde 01/01/2017. Para a preferência tarifária, você precisa de uma prova de origem. O acordo tem um capítulo sobre comércio e desenvolvimento sustentável, com referências às normas fundamentais do trabalho da OIT e a acordos ambientais internacionais.

Na prática, isso significa: confira para cada produto a tarifa e a regra de origem no portal Access2Markets da Comissão Europeia, organizado por código de mercadoria. Muitos produtos agrícolas e industriais estão isentos de tarifas há anos, e para alguns valem cotas ou regras de transição. Para produtos processados, a regra de origem define se houve agregação de valor suficiente no país. Seu importador na UE pode ajudar a emitir a prova de origem corretamente. Guarde a documentação por vários anos, porque a alfândega pode fazer verificações posteriores.

EUDR, CBAM e RGPD valem para produtos e serviços equatorianos independentemente do acordo.

<https://www.mercoeu.com/pt/paises/equador>