

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.

| PROTEÇÃO DE DADOS | ADEQUAÇÃO À UE | ACORDO COM A UE                    | CIBERSEGURANÇA                                                   |
|-------------------|----------------|------------------------------------|------------------------------------------------------------------|
| LOPDP (2021)      | não            | Acordo comercial, desde 01/01/2017 | Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026) |

## 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.

## FAQ

### Com que rapidez uma violação de dados deve ser notificada no Equador?

Em no máximo cinco dias após a violação, à SPDP (art. 43 da LOPDP). Os operadores informam o controlador em até dois dias.

### O Equador tem uma lei de cibersegurança?

Sim. A Ley Orgánica para el Fortalecimiento de la Ciberseguridad está em vigor desde 22/05/2026. Ela visa proteger a infraestrutura crítica e os serviços essenciais.

## Os clientes da UE precisam de cláusulas contratuais padrão para o Equador?

Sim. O Equador não tem decisão de adequação da UE.

## O Acordo UE-Mercosul vale para o Equador?

Não. O Equador é parte, desde 2017, do acordo comercial com a Colômbia e o Peru.

## Qual ferramenta ajuda a responder aos questionários de segurança de clientes da UE?

Para políticas, riscos e evidências de um sistema de gestão conforme a ISO 27001 ou para o RGPD, você pode usar uma plataforma GRC como o [Sightadel](#), que é desenvolvida e hospedada na Alemanha. O [veyrisk](#) verifica de fora o que da sua empresa está acessível pela internet e documenta isso em um relatório.

**Fontes** · Atualizado em: 11 de outubro de 2026

Registro Oficial del Ecuador: <https://www.registroficial.gob.ec/>

Asamblea Nacional: Ley Orgánica para el Fortalecimiento de la Ciberseguridad:

<https://www.asambleanacional.gob.ec/es/node/115246>

EcuCERT: <https://www.ecucert.gob.ec/>

Comissão Europeia, DG Comércio: Comunidade Andina: [https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/andean-community\\_en](https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/andean-community_en)

Comissão Europeia: decisões de adequação: [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

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

### COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



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>