

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.

PROTEÇÃO DE DADOS	ADEQUAÇÃO À UE	ACORDO COM A UE	CIBERSEGURANÇA
Ley Estatutaria 1581 de 2012	não	Acordo comercial, desde 01/08/2013	sem lei; Decreto 338/2022

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.

FAQ

Com que rapidez uma violação de dados deve ser notificada na Colômbia?

Em até 15 dias úteis a partir do conhecimento, pelo Registro Nacional de Bases de Datos, à SIC. Clientes da UE costumam exigir em contrato prazos bem mais curtos.

Os clientes da UE precisam de cláusulas contratuais padrão para a Colômbia?

Sim. A Colômbia não tem decisão de adequação da UE.

A Colômbia tem uma lei como a NIS2?

Não. Existe uma política (CONPES 3995) e o Decreto 338/2022, mas não há obrigações intersetoriais para empresas.

O Acordo UE-Mercosul vale para a Colômbia?

Não. A Colômbia tem um acordo comercial próprio com a UE, aplicado desde 2013.

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

Para a parte técnica, o [veyrisk](#) verifica de fora quais sistemas da sua empresa estão acessíveis pela internet e entrega um relatório que você pode anexar. Políticas, riscos e comprovações organizacionais você pode manter no [Sightadel](#).

Fontes · Atualizado em: 11 de outubro de 2026

Ley Estatutaria 1581 de 2012, Función Pública: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

SIC, Superintendencia de Industria y Comercio: <https://www.sic.gov.co/>

ColCERT: <https://www.colcert.gov.co/>

Comissão Europeia, DG Comércio: Comunidade Andina: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/andean-community_en

Acordo Comercial UE, Colômbia e Peru, EUR-Lex: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22012A1221\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22012A1221(01))

Comissão Europeia: decisões de adequação: 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

**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.

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>