

PAÍS · ASOCIADO AL MERCOSUR

Colombia: lo que esperan los clientes de la UE

Colombia tiene un régimen de protección de datos consolidado y con una autoridad activa, pero no una ley de ciberseguridad. Con la UE rige un acuerdo comercial desde 2013.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
Ley Estatutaria 1581 de 2012	no	Acuerdo Comercial, desde 01/08/2013	sin ley; Decreto 338/2022

Panorama: comercio con la UE

Colombia exporta a la UE sobre todo materias primas y productos agrícolas, entre ellos café del Huila y del Eje Cafetero, banano de Urabá, flores de corte de la Sabana de Bogotá, aguacate y carbón. La página de la Comisión no trae un desglose solo para Colombia. Para el conjunto de los países andinos, menciona para 2025 productos agrícolas (48,7 %), productos minerales (27,1 %) y pesca (13,5 %).

Además crece la exportación de servicios de TI. Equipos de Medellín, Bogotá y Cali desarrollan software y prestan soporte a clientes de España y otros países de la UE.

Protección de datos: la Ley 1581 frente al RGPD

La base es la Ley Estatutaria 1581 de 2012 con sus decretos reglamentarios (Decreto 1377/2013 y Decreto 886/2014, hoy compilados en el Decreto Único 1074/2015). La autoridad es la SIC (Superintendencia de Industria y Comercio), con una delegatura propia de protección de datos. La SIC realiza inspecciones e impone multas.

El derecho colombiano se apoya más en la autorización del titular que el [RGPD \(Reglamento General de Protección de Datos\)](#), que contempla varias bases legales del mismo rango. Las empresas a partir de cierto tamaño tienen que inscribir sus bases de datos en el Registro Nacional de Bases de Datos (RNBD). Allí también se reportan los incidentes de seguridad. Los responsables deben tener políticas escritas de tratamiento de la información, lo que en la práctica se acerca a un esquema de protección de datos según el RGPD.

Colombia no tiene una decisión de adecuación de la UE. Sus clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia. A la inversa, la SIC también controla las transferencias desde Colombia al exterior. Quien mueve datos en ambas direcciones tiene que tener en cuenta los dos regímenes.

Ciberseguridad frente a NIS2

Colombia no tiene una ley de ciberseguridad. La base son el documento de política CONPES 3995 de 2020, sobre confianza y seguridad digital, y el Decreto 338 de 2022, que regula la gobernanza de la seguridad digital. Hace años que se discute una agencia nacional de seguridad digital, pero no se ha creado. El equipo estatal de respuesta es ColCERT, del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Comparado con [NIS2](#), faltan obligaciones transversales de gestión de riesgos y plazos de notificación. El sector financiero está más regulado: la Superintendencia Financiera exige a los bancos y demás entidades vigiladas medidas de ciberseguridad y el reporte de incidentes (Circular Externa 007 de 2018, hoy parte de la Circular Básica Jurídica).

Para los proveedores de clientes europeos, las obligaciones vienen del contrato: cláusulas de NIS2 sobre la cadena de suministro, [DORA](#) si el cliente es del sector financiero y el [Reglamento de Ciberresiliencia \(CRA\)](#) para productos conectados.

Plazos de notificación comparados

MOTIVO	COLOMBIA	UE
Violación de datos ante la autoridad	15 días hábiles desde que se tiene conocimiento, a la SIC a través del RNBD	72 horas (art. 33 RGPD)
Ciberincidente significativo	sin ley general; sector financiero según las normas de la Superintendencia Financiera	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

El plazo colombiano es bastante más largo que el europeo. Si trata datos por encargo de un cliente de la UE, para usted rige el plazo del contrato, por lo general de 24 a 48 horas, para que el cliente pueda cumplir sus 72 horas.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO

Protección de datos	SIC, Superintendencia de Industria y Comercio
Ciberseguridad, CSIRT	MinTIC con ColCERT
Sector financiero	Superintendencia Financiera de Colombia
Acreditación	ONAC, Organismo Nacional de Acreditación de Colombia

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del ONAC o de un organismo extranjero está cubierta por el acuerdo internacional de reconocimiento de la Global ACI (desde el 1 de enero de 2026 sucesora de IAF e ILAC; las acreditaciones existentes siguen reconocidas). En ese caso, el certificado suele ser reconocido por los clientes de la UE. Algunos grupos igual exigen un certificador determinado. Aclárelo antes de invertir en una auditoría.

Lo que suelen exigir los clientes de la UE

Los exportadores de café, cacao y aceite de palma tienen que cumplir el [EUDR](#): geodatos de las fincas, prueba de producción libre de deforestación después del 31/12/2020 y prueba de producción legal. Colombia está clasificada como país de riesgo estándar. Para una cooperativa del Huila con cientos de pequeños productores, reunir los polígonos es el mayor esfuerzo. A los exportadores de banano y flores se les piden certificados como GLOBALG.A.P. o [normas alimentarias](#).

Los proveedores de TI reciben cláusulas contractuales tipo, un cuestionario de seguridad y, a menudo, la pregunta por [ISO 27001](#). Si quiere implementar un sistema de gestión de seguridad de la información, puede llevar políticas, riesgos y evidencias en una plataforma GRC como [Sightadel](#). Para las preguntas del cuestionario sobre sistemas accesibles desde internet, un análisis externo como el de [veyrisk](#) le da una respuesta con evidencia.

En el contrato, estos puntos suelen figurar como anexos: cláusulas contractuales tipo, contrato de encargo del tratamiento, medidas técnicas y organizativas, plazos de notificación y derechos de auditoría. Para la evaluación de impacto de la transferencia, su cliente de la UE pregunta por ubicaciones de almacenamiento, accesos y cifrado. Como en Colombia ya lleva políticas de tratamiento de la información e inscribe sus bases de datos en el RNBD, una parte de las respuestas ya está documentada.

Un punto de partida razonable para empresas colombianas:

1. Aclare cuáles de sus clientes están en la UE y qué normas se les aplican.
2. Compare sus políticas según la Ley 1581 con los requisitos del RGPD, sobre todo en bases legales y plazos de supresión.

3. Reduzca su plazo interno de notificación de incidentes muy por debajo de los 15 días hábiles de la SIC.
4. Para café, cacao y aceite de palma, reúna los geodatos de todas las parcelas, también los de sus proveedores.
5. Evalúe si un certificado ISO 27001 o una norma alimentaria responde muchas preguntas individuales de una sola vez.

En qué punto está hoy se lo muestra el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

Colombia está asociada al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Con la UE rige el Acuerdo Comercial con Colombia, Perú y Ecuador, que se aplica de forma provisional con Colombia desde el 01/08/2013. Para la preferencia arancelaria necesita una prueba de origen. El acuerdo incluye un capítulo sobre comercio y desarrollo sostenible con referencias a las normas fundamentales del trabajo de la OIT y a los acuerdos ambientales internacionales.

En la práctica, esto significa: verifique para cada producto el arancel y la regla de origen en el portal Access2Markets de la Comisión Europea, ordenado por código arancelario. Muchos productos agrícolas e industriales están libres de aranceles desde hace años; para algunos rigen contingentes o reglas transitorias. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en el país. Su importador en la UE puede ayudarle a emitir correctamente la prueba de origen. Conserve los documentos durante varios años, porque la aduana puede hacer controles posteriores.

El derecho de la UE, como el EUDR, el CBAM y el RGPD, se aplica a las mercancías y servicios colombianos con independencia del acuerdo.

FAQ

¿En cuánto tiempo hay que reportar una violación de datos en Colombia?

Dentro de los 15 días hábiles desde que se tiene conocimiento, a la SIC a través del Registro Nacional de Bases de Datos. Los clientes de la UE suelen exigir por contrato plazos mucho más cortos.

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

Sí. Colombia no tiene una decisión de adecuación de la UE.

¿Tiene Colombia una ley como NIS2?

No. Hay una política (CONPES 3995) y el Decreto 338/2022, pero no obligaciones transversales para las empresas.

¿Rige el Acuerdo UE-Mercosur para Colombia?

No. Colombia tiene su propio acuerdo comercial con la UE, aplicado desde 2013.

¿Qué herramienta ayuda a preparar ISO 27001 desde Colombia?

Una plataforma GRC con plantillas y control de avance. [Sightadel](#) guía capítulo por capítulo a través de la norma, funciona en español y se aloja en Alemania. La auditoría la hace después un organismo de certificación acreditado; Sightadel no emite certificados.

Fuentes · Actualizado: 11 de octubre 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/>

Comisión Europea, DG Comercio: Comunidad Andina: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/andean-community_en

Acuerdo Comercial UE, Colombia y Perú, 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))

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

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por NIS2: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)



veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)



Valar es un firewall de hardware con software de neonotu. Protege oficinas y sedes y genera los registros que exigen NIS2 e ISO 27001.

[Ver Valar →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

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