

PAÍS · ASOCIADO AL MERCOSUR

Ecuador: lo que esperan los clientes de la UE

Ecuador tiene desde 2021 una ley de protección de datos inspirada en el modelo europeo y, desde mayo de 2026, una ley para el fortalecimiento de la ciberseguridad. Con la UE lo une un acuerdo comercial desde 2017.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
LOPDP (2021)	no	Acuerdo Comercial, desde 01/01/2017	Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026)

Panorama: comercio con la UE

Ecuador envía a Europa sobre todo alimentos: banano de El Oro y Los Ríos, camarón del golfo de Guayaquil, atún en conserva de Manta, cacao y flores de corte de la Sierra. La Comisión publica cifras solo para el conjunto de los países andinos. En 2025, el 48,7 % correspondió a productos agrícolas, el 27,1 % a productos minerales y el 13,5 % a la pesca, un rubro en el que Ecuador es especialmente fuerte.

Para los exportadores de cacao y aceite de palma rige el [EUDR](#). Las empresas pesqueras y alimentarias necesitan además la habilitación de la UE para alimentos de origen animal y certificados alimentarios sólidos.

Protección de datos: la LOPDP frente al RGPD

La Ley Orgánica de Protección de Datos Personales (LOPDP) se publicó en mayo de 2021 en el Registro Oficial. Tras un período de transición de dos años, desde mayo de 2023 rigen también las sanciones. El reglamento es el Decreto Ejecutivo 904 de 2023. La autoridad de control es la Superintendencia de Protección de Datos Personales (SPDP).

La LOPDP sigue de cerca al [RGPD \(Reglamento General de Protección de Datos\)](#): bases de legitimación, derechos de los titulares, delegados de protección de datos, evaluaciones de impacto, obligaciones de los encargados y reglas para las transferencias internacionales. Quien conoce el RGPD se orienta rápido.

La diferencia está en el plazo de notificación de vulneraciones: el art. 43 de la LOPDP exige notificar a la SPDP a más tardar cinco días después de la vulneración. Los encargados tienen que informar al

responsable dentro de los dos días. La notificación se hace mediante un sistema electrónico de la SPDP.

Ecuador 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.

Ciberseguridad frente a NIS2

Desde el 22/05/2026 rige la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada en el Registro Oficial. Su objetivo declarado es proteger la infraestructura crítica y asegurar la continuidad de los servicios esenciales. Crea un Sistema Nacional de Ciberseguridad y reforma siete leyes vigentes, entre ellas la LOPDP y la ley de telecomunicaciones. En el centro están las entidades públicas y los operadores de infraestructura crítica.

El enfoque se parece al de [NIS2](#), que apunta a entidades esenciales e importantes de 18 sectores. Si su empresa está alcanzada, qué obligaciones de gestión de riesgos rigen y en qué plazo hay que notificar los incidentes es algo que conviene verificar en el texto de la ley publicado en el Registro Oficial y en su normativa de aplicación. Una empresa que ya trabaja según [ISO 27001](#) va a tener cubierta la mayoría de los requisitos.

Para los proveedores de clientes europeos rigen, con independencia de eso, los requisitos contractuales: 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	ECUADOR	UE
Violación de datos ante la autoridad	a más tardar 5 días después de la vulneración, ante la SPDP (art. 43 LOPDP)	72 horas (art. 33 RGPD)
Encargado al responsable	2 días	sin dilación indebida (art. 33, apdo. 2 RGPD)
Ciberincidente significativo	ley vigente desde el 22/05/2026; verificar plazo y organismo receptor en el texto del Registro Oficial	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Si trata datos por encargo de un cliente de la UE, rige el plazo del contrato, por lo general de 24 a 48 horas. Los dos días que la LOPDP da a los encargados normalmente no alcanzan para eso.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	SPDP, Superintendencia de Protección de Datos Personales
CSIRT	EcuCERT de la ARCOTEL
Sector financiero	Superintendencia de Bancos
Acreditación	SAE, Servicio de Acreditación Ecuatoriano

En cuanto a los certificados, importa menos dónde está el organismo certificador que quién lo acreditó. Antes de contratarlo, pregunte si la acreditación del SAE 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.

Qué organismo recibe las notificaciones bajo la nueva ley de ciberseguridad conviene verificarlo directamente en el texto de la ley o con su ente de control sectorial.

Lo que suelen exigir los clientes de la UE

Un camaronero de El Oro que vende a un mayorista en España necesita la habilitación de su establecimiento para el mercado de la UE, trazabilidad hasta la piscina y, por lo general, un certificado [IFS](#), [BRCGS](#) o [FSSC 22000](#). A los exportadores de banano y flores se les pide GLOBALG.A.P. Los exportadores de cacao tienen que entregar, para el EUDR, los geodatos de las parcelas y la prueba de producción libre de deforestación después del 31/12/2020. Ecuador está clasificado como país de riesgo estándar.

Los proveedores de TI reciben cláusulas contractuales tipo, cuestionarios de seguridad y la pregunta por [ISO 27001](#). Quien implementa un sistema de gestión según ISO 27001 puede llevar políticas, riesgos y evidencias en una plataforma GRC como [Sightadel](#). Para las preguntas sobre sistemas accesibles desde internet sirve un análisis externo, por ejemplo con [veyrisk](#), cuyo informe puede adjuntar a la respuesta.

En el contrato, estos puntos suelen figurar en 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. La LOPDP le da una buena base para eso, porque adopta muchos conceptos y obligaciones del RGPD.

Un punto de partida razonable para empresas ecuatorianas:

1. Verifique si queda alcanzado por la ley de ciberseguridad de 2026.
2. Compare su documentación según la LOPDP con los requisitos del RGPD. Las brechas suelen ser pequeñas.
3. Reduzca su plazo interno de notificación de incidentes muy por debajo de los cinco días de la LOPDP.
4. Para cacao y aceite de palma, reúna los geodatos de todas las parcelas, también los de sus proveedores.
5. Mantenga al día las habilitaciones, la trazabilidad y los certificados alimentarios para camarón, atún y banano.

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

Acuerdo con la UE

Ecuador está asociado al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Se adhirió al Acuerdo Comercial de la UE con Colombia y Perú, que se aplica desde el 01/01/2017. 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 EUDR, el CBAM y el RGPD se aplican a las mercancías y servicios ecuatorianos con independencia del acuerdo.

FAQ

¿En cuánto tiempo hay que notificar una violación de datos en Ecuador?

A más tardar cinco días después de la vulneración, ante la SPDP (art. 43 LOPDP). Los encargados informan al responsable dentro de los dos días.

¿Tiene Ecuador una ley de ciberseguridad?

Sí. La Ley Orgánica para el Fortalecimiento de la Ciberseguridad rige desde el 22/05/2026. Apunta a proteger la infraestructura crítica y los servicios esenciales.

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

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

¿Rige el Acuerdo UE-Mercosur para Ecuador?

No. Desde 2017, Ecuador es parte del Acuerdo Comercial con Colombia y Perú.

¿Qué herramienta ayuda a documentar la LOPDP y el RGPD a la vez?

Como la LOPDP sigue de cerca al RGPD, buena parte de la documentación sirve para ambos.

[Sightadel](#) trae el RGPD como marco, con plantillas para el registro de actividades de tratamiento, las medidas técnicas y organizativas y el proceso de notificación. Lo que la LOPDP pide en forma adicional, como el plazo de cinco días ante la SPDP, lo agrega usted.

Fuentes · Actualizado: 11 de octubre 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/>

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

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>