

PAÍS · ASOCIADO AL MERCOSUR

Perú: lo que esperan los clientes de la UE

En 2025, Perú modernizó su régimen de protección de datos y exige notificar los incidentes de seguridad dentro de las 48 horas. Desde fines de 2025, los servicios digitales de sectores clave tienen además la obligación de notificar al centro nacional de seguridad digital.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
Ley 29733, DS 016-2024-JUS	no	Acuerdo Comercial, desde 01/03/2013	DU 007-2020, DS 126-2025-PCM

Panorama: comercio con la UE

Perú exporta a la UE sobre todo productos mineros y agrícolas: concentrados de cobre y zinc de los Andes, arándanos, paltas y uvas de la costa, café de Cajamarca y Junín, además de harina de pescado. La Comisión publica las 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.

Para los exportadores de café y cacao, el [EUDR](#) es la obligación nueva más importante. A las empresas mineras se les pregunta sobre todo por medio ambiente, condiciones laborales y emisiones.

Protección de datos: la Ley 29733 frente al RGPD

La base es la Ley Nº 29733 de Protección de Datos Personales, de 2011. El nuevo reglamento, Decreto Supremo Nº 016-2024-JUS, está vigente desde el 30/03/2025 y reemplaza al reglamento anterior de 2013. Acerca bastante el derecho peruano al [RGPD \(Reglamento General de Protección de Datos\)](#): oficial de datos personales para ciertos titulares de bancos de datos, obligaciones en los flujos transfronterizos, reglas para los encargados del tratamiento y, sobre todo, un plazo fijo para notificar incidentes de seguridad. La autoridad es la Autoridad Nacional de Protección de Datos Personales (ANPD), del Ministerio de Justicia y Derechos Humanos.

Con 48 horas, el plazo de notificación es más corto que las 72 horas del RGPD. Los especialistas interpretan de distinta manera en qué momento exacto corresponde notificar. Ante la duda, mejor notifique. Un proveedor peruano que trata datos por encargo de un cliente de la UE tiene que ser rápido, entonces, tanto con su cliente como con la ANPD.

Perú no tiene una decisión de adecuación de la UE. Los clientes de la UE necesitan cláusulas contractuales tipo y una evaluación de impacto de la transferencia.

Ciberseguridad frente a NIS2

Con la Ley Nº 30999 (Ley de Ciberdefensa) de 2019, Perú tiene una ley de ciberdefensa del Estado. Regula las funciones de las Fuerzas Armadas y del Estado, no las obligaciones de las empresas. Una ley de ciberseguridad que, como NIS2, imponga obligaciones a las empresas no existe; en el Congreso solo hay proyectos. La base es el Marco de Confianza Digital (Decreto de Urgencia Nº 007-2020) junto con la Ley de Gobierno Digital (Decreto Legislativo 1412). Su reglamento, el Decreto Supremo Nº 126-2025-PCM, se publicó en noviembre de 2025. Según este, los proveedores de servicios digitales en sectores como finanzas, servicios básicos, salud, transporte, acceso a internet y educación tienen que notificar los incidentes críticos al Centro Nacional de Seguridad Digital (CNSD).

El enfoque se parece al de [NIS2](#): obligaciones para sectores clave, un punto central de notificación y plazos cortos. NIS2 va más allá, por ejemplo en las obligaciones de gestión de riesgos, de cadena de suministro y de responsabilidad personal de la dirección. Los bancos y las aseguradoras tienen además sus propias exigencias de seguridad de la información y ciberseguridad fijadas por la SBS.

Para los proveedores de clientes europeos se suman 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	PERÚ	UE
Violación de datos ante la autoridad	48 horas desde que se tiene conocimiento, ante la ANPD (DS 016-2024-JUS)	72 horas (art. 33 RGPD)
Incidente crítico en servicios digitales	48 horas ante el CNSD (DS 126-2025-PCM)	24 h alerta temprana, 72 h notificación, informe final al mes (art. 23 NIS2)

Un incidente con datos personales puede dar lugar a las dos notificaciones, ante la ANPD y ante el CNSD. Téngalo previsto en su proceso, con un responsable claro para cada notificación.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	ANPD, Ministerio de Justicia y Derechos Humanos

ÁREA	ORGANISMO
Seguridad digital	Secretaría de Gobierno y Transformación Digital (PCM)
CSIRT	Centro Nacional de Seguridad Digital con PeCERT
Sector financiero	SBS, Superintendencia de Banca, Seguros y AFP
Acreditación	INACAL, Instituto Nacional de Calidad

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

Un exportador de café de Junín necesita, para el EUDR, los geodatos de todas las parcelas de sus proveedores y la prueba de que allí no hubo deforestación después del 31/12/2020. Perú está clasificado como país de riesgo estándar. A los exportadores de fruta se les pide [IFS](#), [BRCGS](#) o [FSSC 22000](#) y GLOBALG.A.P.; a las empresas mineras, con frecuencia, [ISO 14001](#).

Los proveedores de TI y de outsourcing reciben cláusulas contractuales tipo, cuestionarios de seguridad y la pregunta por [ISO 27001](#). Las políticas, los riesgos y las evidencias que piden esos cuestionarios se pueden llevar en una plataforma GRC como [Sightadel](#). Muchos clientes de la UE revisan también qué sistemas de sus proveedores están expuestos en internet. Con [veyrisk](#) usted ve esa superficie de ataque antes de que el cliente pregunte.

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. Aquí le ayuda que el derecho peruano, con el nuevo reglamento, ya contemple un plazo de notificación corto y obligaciones para los encargados.

Un punto de partida razonable para empresas peruanas:

1. Verifique si, como proveedor de servicios digitales, queda alcanzado por el DS 126-2025-PCM.
2. Compare su documentación según el DS 016-2024-JUS con los requisitos del RGPD.
3. Arme un proceso de notificación que atienda a la ANPD, al CNSD y a sus clientes de la UE dentro del mismo plazo.

4. Para café y cacao, reúna los geodatos de todas las parcelas, también los de sus proveedores.
5. Verifique qué certificado piden sus clientes con más frecuencia y planifique la auditoría con un organismo reconocido.

Un primer panorama se lo da el [EU-Readiness-Check](#) gratuito.

Acuerdo con la UE

Perú está asociado 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 Perú desde el 01/03/2013. Para la preferencia arancelaria necesita una prueba de origen. El capítulo sobre comercio y desarrollo sostenible remite 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 peruanos con independencia del acuerdo.

FAQ

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

Dentro de las 48 horas desde que se tiene conocimiento, ante la ANPD, según el reglamento DS 016-2024-JUS, vigente desde el 30/03/2025.

¿Quién tiene que notificar incidentes al CNSD?

Los proveedores de servicios digitales en sectores clave como finanzas, salud, transporte o servicios básicos, en caso de incidentes críticos, dentro de las 48 horas (DS 126-2025-PCM).

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

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

¿Rige el Acuerdo UE-Mercosur para Perú?

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

¿Qué herramienta ayuda a responder los cuestionarios de seguridad de clientes de la UE?

Para la parte organizativa, una plataforma GRC: en [Sightadel](#) se arma un sistema de gestión según ISO 27001 o NIS2 con plantillas, y los datos quedan en la UE. Para las preguntas técnicas sobre lo que está expuesto en internet, el [informe de veyrisk](#) muestra servicios abiertos, certificados y vulnerabilidades vistos desde afuera.

Fuentes · Actualizado: 11 de octubre de 2026

ANPD Perú: <https://www.gob.pe/anpd>

DS 016-2024-JUS, gob.pe (texto oficial): <https://www.gob.pe/institucion/smv/normas-legales/6426760-016-2024-jus>

El Peruano: Incidente de seguridad digital o de datos personales: <https://elperuano.pe/noticia/292188-incidente-de-seguridad-digital-o-de-datos-personales>

PCM: Normas legales: <https://www.gob.pe/institucion/pcm/normas-legales>

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>