

PAÍS · ASSOCIADO AO MERCOSUL

Peru: o que os clientes da UE esperam

O Peru modernizou sua legislação de proteção de dados em 2025 e exige a notificação de violações de dados em até 48 horas. Desde o fim de 2025, serviços digitais em setores importantes também têm de notificar incidentes ao centro nacional de segurança digital.

PROTEÇÃO DE DADOS	ADEQUAÇÃO À UE	ACORDO COM A UE	CIBERSEGURANÇA
Ley 29733, DS 016-2024-JUS	não	Acordo comercial, desde 01/03/2013	DU 007-2020, DS 126-2025-PCM

Visão geral: comércio com a UE

O Peru exporta para a UE principalmente produtos da mineração e do agro: concentrados de cobre e zinco dos Andes, mirtilos, abacates e uvas do litoral, café de Cajamarca e Junín, além de farinha de peixe. 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.

Para exportadores de café e cacau, a [EUDR](#) é a maior obrigação nova. Mineradoras recebem perguntas sobretudo sobre meio ambiente, condições de trabalho e emissões.

Proteção de dados: Ley 29733 e o RGPD

A base é a Ley Nº 29733, de 2011, sobre proteção de dados pessoais. O novo regulamento, o Decreto Supremo Nº 016-2024-JUS, está em vigor desde 30/03/2025 e substitui o regulamento anterior, de 2013. Ele aproxima bastante o direito peruano do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): encarregados de proteção de dados para determinados controladores, obrigações nas transferências internacionais, regras para operadores e, principalmente, um prazo fixo para notificar violações de dados. A autoridade de controle é a Autoridad Nacional de Protección de Datos Personales (ANPD), ligada ao Ministério da Justiça. Atenção para não confundir com a ANPD brasileira, que tem a mesma sigla.

Com 48 horas, o prazo de notificação é mais curto que as 72 horas do RGPD. Especialistas interpretam de formas diferentes quando exatamente a notificação passa a ser devida. Na dúvida, notifique. Um prestador de serviços peruano que trata dados para um cliente da UE precisa, portanto, ser rápido tanto com o cliente quanto com a ANPD.

O Peru não tem decisão de adequação da UE. Os clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência.

Cibersegurança comparada à NIS2

Com a Ley Nº 30999 (Ley de Ciberdefensa), de 2019, o Peru tem uma lei de ciberdefesa do Estado. Ela trata das funções das Forças Armadas e do Estado, não de obrigações para empresas. Uma lei de cibersegurança que, como a NIS2, imponha deveres às empresas não existe. No Congresso há apenas projetos. A base é o Marco de Confianza Digital (Decreto de Urgencia Nº 007-2020), junto com a lei de governo digital (Decreto Legislativo 1412). O regulamento correspondente, o Decreto Supremo Nº 126-2025-PCM, foi publicado em novembro de 2025. Por ele, prestadores de serviços digitais em setores como finanças, serviços básicos, saúde, transporte, acesso à internet e educação devem notificar incidentes críticos ao Centro Nacional de Seguridad Digital (CNSD).

A abordagem lembra a da [NIS2](#): obrigações para setores importantes, um ponto central de notificação e prazos curtos. A NIS2 vai além, por exemplo nas obrigações de gestão de riscos, na cadeia de suprimentos e na responsabilidade pessoal da alta direção. Bancos e seguradoras têm ainda normas próprias do órgão supervisor SBS sobre segurança da informação e cibersegurança.

Para fornecedores de clientes europeus, somam-se as exigências contratuais: 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	PERU	UE
Violação de dados à autoridade	48 horas a partir do conhecimento, à ANPD (DS 016-2024-JUS)	72 horas (art. 33 do RGPD)
Incidente crítico em serviços digitais	48 horas, ao CNSD (DS 126-2025-PCM)	24 h para o alerta precoce, 72 h para a notificação, relatório final após um mês (art. 23 da NIS2)

Um incidente com dados pessoais pode gerar as duas notificações, à ANPD e ao CNSD. Preveja isso no seu processo, com um responsável definido para cada notificação.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO

Proteção de dados	ANPD, Ministerio de Justicia y Derechos Humanos
Segurança digital	Secretaría de Gobierno y Transformación Digital (PCM)
CSIRT	Centro Nacional de Seguridad Digital com o PeCERT
Setor financeiro	SBS, Superintendencia de Banca, Seguros y AFP
Acreditação	INACAL, Instituto Nacional de Calidad

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 INACAL 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

Um exportador de café de Junín precisa, para a EUDR, da geolocalização de todas as parcelas dos seus fornecedores e da comprovação de que não houve desmatamento ali após 31/12/2020. O Peru está classificado como país de risco padrão. Exportadores de frutas são questionados sobre [IFS](#), [BRCGS](#) ou [FSSC 22000](#) e GLOBALG.A.P., e mineradoras, com frequência, sobre a [ISO 14001](#).

Prestadores de serviços de TI e de outsourcing recebem cláusulas contratuais padrão, questionários de segurança e a pergunta sobre a [ISO 27001](#). Muitos clientes da UE também verificam quais sistemas dos seus fornecedores estão expostos na internet. Com o [veyrisk](#) você mesmo vê essa superfície de ataque antes que o cliente pergunte.

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. Aqui ajuda o fato de o direito peruano, com o novo regulamento, já prever um prazo curto de notificação e obrigações para operadores. As medidas técnicas e organizacionais e as comprovações para esses anexos podem ser organizadas no [Sightadel](#), que é desenvolvido e hospedado na Alemanha.

Um bom ponto de partida para empresas peruanas:

1. Verifique se sua empresa, como prestadora de serviços digitais, está sujeita ao DS 126-2025-PCM.
2. Compare sua documentação segundo o DS 016-2024-JUS com os requisitos do RGPD.

3. Monte um processo de notificação que atenda a ANPD, o CNSD e seus clientes na UE dentro do mesmo prazo.
4. Para café e cacau, reúna a geolocalização de todas as parcelas, inclusive as dos seus fornecedores.
5. Veja qual certificado seus clientes pedem com mais frequência e planeje a auditoria com um organismo reconhecido.

Uma primeira visão geral está no [Diagnóstico UE](#) gratuito.

Acordo com a UE

O Peru é associado 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 o Peru desde 01/03/2013. Para a preferência tarifária, você precisa de uma prova de origem. O capítulo sobre comércio e desenvolvimento sustentável faz referência 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 peruanos independentemente do acordo.

FAQ

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

Em até 48 horas a partir do conhecimento, à ANPD, conforme o regulamento DS 016-2024-JUS, em vigor desde 30/03/2025.

Quem precisa notificar incidentes ao CNSD?

Prestadores de serviços digitais em setores importantes, como finanças, saúde, transporte ou serviços básicos, em até 48 horas no caso de incidentes críticos (DS 126-2025-PCM).

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

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

O Acordo UE-Mercosul vale para o Peru?

Não. O Peru tem um acordo comercial próprio com a UE, aplicado desde 2013.

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

O [veyrisk](#) verifica de fora quais sistemas da sua empresa estão acessíveis pela internet e entrega um relatório que você pode usar como comprovação. Para a documentação conforme a ISO 27001 ou o RGPD, o [Sightadel](#) organiza tarefas, comprovações e a preparação da auditoria.

Fontes · Atualizado em: 11 de outubro 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>

Comissão Europeia, DG Comércio: Comunidade Andina: 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

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>