

PAÍS · ASSOCIADO AO MERCOSUL

Chile: o que os clientes da UE esperam

O Chile tem a lei de cibersegurança mais próxima da NIS2 na região e uma nova lei de proteção de dados que deve entrar em vigor em 01/12/2026. Desde fevereiro de 2025, o país está ligado à UE por um acordo comercial modernizado.

PROTEÇÃO DE DADOS	ADEQUAÇÃO À UE	ACORDO COM A UE	CIBERSEGURANÇA
Ley 21.719, em vigor a partir de 01/12/2026	não	Acordo comercial provisório desde 01/02/2025	Ley 21.663, Marco de Ciberseguridad

Visão geral: comércio com a UE

Segundo a Comissão Europeia, as importações da UE vindas do Chile em 2025 foram compostas em 40% por produtos vegetais, em 20% por produtos minerais e em 20% por metais comuns. Por trás desses números estão frutas e vinhos do Vale Central, o cobre de Antofagasta e o lítio do Atacama. O cobre, aliás, não está no [CBAM](#). Aço, alumínio e fertilizantes estão.

Santiago também é um polo importante de prestadores de serviços de TI, data centers e fintechs que atendem clientes na Espanha e em outros países da UE.

Proteção de dados: Ley 21.719 e o RGPD

A Ley 21.719 reforma a fundo a antiga lei de proteção de dados, a Ley 19.628. Ela foi publicada no Diário Oficial em 13/12/2024 e entra em vigor em 01/12/2026. A lei adota muitos elementos do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais, direitos ampliados dos titulares, incluindo a portabilidade, obrigações para operadores, regras para transferências ao exterior e o dever de notificar incidentes de segurança. A novidade é uma autoridade de controle própria, a Agencia de Protección de Datos Personales, com poder para aplicar multas.

Possível adiamento: em 31/08/2026 o governo apresentou o projeto de lei Boletín 18.623-07. Ele adiará a entrada em vigor para 01/12/2027 e ampliará o conselho da agência. Em 11/10/2026 o projeto ainda não tinha sido aprovado, portanto continua valendo a data de 01/12/2026.

O Chile não tem decisão de adequação da UE. Seus clientes europeus precisam de cláusulas contratuais padrão e de uma avaliação de impacto da transferência para enviar dados ao Chile.

Cibersegurança comparada à NIS2

A Ley 21.663, Ley Marco de Ciberseguridad, foi publicada em abril de 2024. A agência nacional de cibersegurança, a ANCI, funciona desde 01/01/2025, e as demais disposições valem desde 01/03/2025. Assim como a [NIS2](#), a lei distingue dois grupos: prestadores de serviços essenciais e operadores de importância vital (Operadores de Importancia Vital, OIV). Ambos precisam notificar ao CSIRT Nacional os incidentes com impacto significativo. Os OIV têm ainda obrigações sobre sistemas de gestão, planos de contingência e auditorias.

Nos prazos, o Chile é mais rígido que a UE. O alerta precoce tem de chegar em até três horas, enquanto a NIS2 pede 24 horas. Os detalhes estão no Reglamento de Reporte de Incidentes (Decreto 295/2024).

No setor financeiro valem também as normas da comissão do mercado financeiro, a CMF, sobre segurança da informação, cibersegurança e notificação de incidentes operacionais. Quem fornece para bancos ou seguradoras europeus recebe, além disso, cláusulas da [DORA](#).

Prazos de notificação comparados

SITUAÇÃO	CHILE	UE
Alerta precoce de incidente cibernético	3 horas a partir do conhecimento (Ley 21.663)	24 horas (art. 23 da NIS2)
Atualização	72 horas; OIV com serviço essencial afetado, 24 horas	72 horas
Relatório final	15 dias corridos a partir do alerta precoce	um mês
Plano de ação dos OIV	no máximo 7 dias corridos	sem equivalente
Violação de dados à autoridade	dever de notificação pela Ley 21.719 a partir da entrada em vigor	72 horas (art. 33 do RGPD)

Quem cumpre os prazos chilenos também cumpre os da NIS2. Um processo de notificação pensado para três horas não precisa de uma segunda versão para clientes da UE.

Autoridades, CSIRT e organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	Agencia de Protección de Datos Personales (nova, criada pela Ley 21.719)

ÁREA	ÓRGÃO
Cibersegurança	ANCI, Agencia Nacional de Ciberseguridad
CSIRT	CSIRT Nacional, vinculado à ANCI
Setor financeiro	CMF, Comisión para el Mercado Financiero
Acreditação	INN, Instituto Nacional de Normalización

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 INN 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 frutas e vinhos são questionados sobre segurança de alimentos, em geral com certificados [IFS](#), [BRCGS](#) ou [FSSC 22000](#) ou GLOBALG.A.P. Madeira e celulose entram na [EUDR](#). Lá o Chile está classificado como país de baixo risco, então a diligência devida é simplificada, mas não dispensável. Mineradoras recebem perguntas sobre meio ambiente, direitos humanos e emissões, muitas vezes com referência à [ISO 14001](#).

Prestadores de serviços de TI e data centers são questionados sobre a [ISO 27001](#). Quem já está sujeito à Ley 21.663 como OIV ou prestador de serviços essenciais já montou o processo de notificação e o sistema de gestão e pode usar isso como comprovação perante clientes da UE. Uma plataforma GRC como o [Sightadel](#), que traz a NIS2 e a ISO 27001 como marcos próprios, ajuda a manter essas comprovações organizadas. Muitos clientes também verificam seus sistemas acessíveis pela internet. Com o [veyrisk](#) você mesmo acompanha essa superfície de ataque.

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. Com a Ley 21.719 e uma autoridade de proteção de dados própria, você poderá apontar um marco legal mais próximo do europeu.

Um bom ponto de partida para empresas chilenas:

1. Verifique se sua empresa está sujeita à Ley 21.663, como prestadora de serviços essenciais ou como OIV.
2. Prepare-se para a Ley 21.719 como se a data de 01/12/2026 fosse certa. O que você fizer para isso, seus clientes na UE já esperam de qualquer forma.
3. Reúna em um único fluxo as notificações para a ANCI, para a nova agência de proteção de dados e para seus clientes na UE.
4. Para madeira, celulose e outros produtos da EUDR, verifique com seu comprador a diligência devida simplificada.
5. Para aço, alumínio e fertilizantes, esclareça quais dados de emissões seu importador precisa para o CBAM.

Uma visão rápida da sua situação está no [Diagnóstico UE](#) gratuito.

Acordo com a UE

O Chile é associado ao Mercosul, mas não faz parte do Acordo UE-Mercosul. Tem um conjunto próprio de tratados com a UE: o Advanced Framework Agreement e o Acordo Comercial Provisório, ambos assinados em 13/12/2023. O Acordo Comercial Provisório está em vigor desde 01/02/2025 e substitui a parte comercial do Acordo de Associação de 2002. Ele traz, entre outros, capítulos sobre energia e matérias-primas e sobre desenvolvimento sustentável. Para a preferência tarifária, você precisa de uma declaração de origem.

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. A maior parte do comércio entre o Chile e a UE é isenta de tarifas. Para produtos processados, a regra de origem define se houve agregação de valor suficiente no Chile. Para lítio e cobre, o acordo tem regras próprias sobre matérias-primas e energia. Seu importador na UE pode ajudar a emitir a declaração de origem corretamente. Guarde os comprovantes por vários anos, porque a alfândega pode fazer verificações posteriores.

Mesmo com o acordo, EUDR, CBAM e RGPD continuam valendo da mesma forma para produtos e serviços chilenos.

FAQ

Quando entra em vigor a nova lei de proteção de dados do Chile?

A Ley 21.719 entra em vigor em 01/12/2026. O projeto Boletín 18.623-07 adiará a data para 01/12/2027, mas ainda não foi aprovado (situação em 11/10/2026).

Com que rapidez um incidente cibernético deve ser notificado no Chile?

Alerta precoce em até 3 horas ao CSIRT Nacional, atualização em até 72 horas (OIV, 24 horas) e relatório final em até 15 dias a partir do alerta precoce.

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

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

O cobre chileno está sujeito ao CBAM?

Não. O cobre não está entre os produtos do CBAM. Mais detalhes na página sobre o [CBAM](#).

Qual ferramenta ajuda a se preparar para a Ley 21.719?

Como a Ley 21.719 adota muitos elementos do RGPD, um programa de proteção de dados montado segundo o RGPD cobre boa parte dela. O [Sightadel](#) traz o RGPD como marco, com modelos, tarefas e comprovações, e é desenvolvido e hospedado na Alemanha.

Fontes · Atualizado em: 11 de outubro de 2026

Ley 21.663, Ley Chile (BCN): <https://www.bcn.cl/leychile/navegar?idNorma=1202434>

ANCI: Plazos para reportar: <https://soporte.anci.gob.cl/hc/anci/articles/1740428298-plazos-para-reportar>

ANCI, Agencia Nacional de Ciberseguridad: <https://anci.gob.cl/>

Senado de Chile (Boletín 18.623-07): <https://www.senado.cl/>

Comissão Europeia, DG Comércio: Chile: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/chile_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>