

PAÍS · ASOCIADO AL MERCOSUR

Chile: lo que esperan los clientes de la UE

Chile tiene la ley de ciberseguridad más cercana a NIS2 en la región y una nueva ley de protección de datos que debe entrar en vigor el 01/12/2026. Desde febrero de 2025 lo une a la UE un acuerdo comercial modernizado.

PROTECCIÓN DE DATOS	ADECUACIÓN DE LA UE	ACUERDO CON LA UE	CIBERSEGURIDAD
Ley 21.719, vigente desde 01/12/2026	no	Acuerdo Comercial Interino desde 01/02/2025	Ley 21.663, Ley Marco de Ciberseguridad

Panorama: comercio con la UE

Según la Comisión Europea, en 2025 las importaciones de la UE desde Chile fueron en un 40 % productos vegetales, en un 20 % productos minerales y en otro 20 % metales comunes. Detrás de esas cifras están la fruta y el vino del Valle Central, pero también el cobre de Antofagasta y el litio de Atacama. Vale aclarar que el cobre no está incluido en el [CBAM](#); el acero, el aluminio y los fertilizantes, en cambio, sí.

Santiago es además un polo importante de proveedores de TI, centros de datos y fintechs que también atienden a clientes en España y otros países de la UE.

Protección de datos: la Ley 21.719 frente al RGPD

La Ley 21.719 reforma a fondo la antigua ley de protección de datos, la Ley 19.628. Se publicó el 13/12/2024 en el Diario Oficial y entra en vigor el 01/12/2026. La ley incorpora muchos elementos del [RGPD \(Reglamento General de Protección de Datos\)](#): bases de licitud, derechos ampliados de los titulares, incluida la portabilidad, obligaciones para los encargados, reglas para las transferencias internacionales y la obligación de notificar vulneraciones de seguridad. Lo nuevo es una autoridad de control propia, la Agencia de Protección de Datos Personales, con facultades para aplicar multas.

Posible aplazamiento: el 31/08/2026, el Gobierno ingresó el proyecto de ley Boletín 18.623-07. Este postergaría la entrada en vigor al 01/12/2027 y ampliaría el consejo de la Agencia. Al 11/10/2026 no ha sido aprobado, por lo que sigue rigiendo el 01/12/2026.

Chile 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 para enviar datos a Chile.

Ciberseguridad frente a NIS2

La Ley 21.663, Ley Marco de Ciberseguridad, se publicó en abril de 2024. La Agencia Nacional de Ciberseguridad (ANCI) funciona desde el 01/01/2025 y las demás disposiciones rigen desde el 01/03/2025. Al igual que [NIS2](#), la ley distingue dos grupos: los prestadores de servicios esenciales y los Operadores de Importancia Vital (OIV). Ambos tienen que notificar al CSIRT Nacional los incidentes con efectos significativos; los OIV tienen además obligaciones sobre sistemas de gestión, planes de continuidad y auditorías.

En los plazos, Chile es más estricto que la UE. La alerta temprana tiene que enviarse dentro de las tres horas; NIS2 la exige dentro de las 24 horas. Los detalles los regula el Reglamento de Reporte de Incidentes (Decreto 295/2024).

En el sector financiero rigen además las normas de la Comisión para el Mercado Financiero (CMF) sobre seguridad de la información y ciberseguridad y sobre la notificación de incidentes operacionales. Quien provee a bancos o aseguradoras europeos recibe, además, cláusulas de [DORA](#).

Plazos de notificación comparados

MOTIVO	CHILE	UE
Alerta temprana de ciberincidente	3 horas desde que se tiene conocimiento (Ley 21.663)	24 horas (art. 23 NIS2)
Actualización	72 horas; 24 horas para OIV con un servicio esencial afectado	72 horas
Informe final	15 días corridos desde la alerta temprana	un mes
Plan de acción OIV	como máximo 7 días corridos	sin equivalente
Vulneración de datos ante la autoridad	obligación de notificar según la Ley 21.719 desde su entrada en vigor	72 horas (art. 33 RGPD)

Quien cumple los plazos chilenos cumple también los de NIS2. Un proceso de notificación pensado para tres horas no necesita, entonces, una segunda versión para los clientes de la UE.

Autoridades, CSIRT, organismo de acreditación

ÁREA	ORGANISMO
Protección de datos	Agencia de Protección de Datos Personales (nueva con la Ley 21.719)

ÁREA	ORGANISMO
Ciberseguridad	ANCI, Agencia Nacional de Ciberseguridad
CSIRT	CSIRT Nacional de la ANCI
Sector financiero	CMF, Comisión para el Mercado Financiero
Acreditación	INN, Instituto Nacional de Normalización

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

A los exportadores de fruta y vino se les pregunta por inocuidad alimentaria, por lo general con certificados [IFS](#), [BRCGS](#) o [FSSC 22000](#) o GLOBALG.A.P. La madera y la celulosa quedan alcanzadas por el [EUDR](#). Ahí Chile está clasificado como país de riesgo bajo, de modo que la diligencia debida es simplificada, pero no prescindible. Las empresas mineras reciben preguntas sobre medio ambiente, derechos humanos y emisiones, a menudo con referencia a [ISO 14001](#).

A los proveedores de TI y centros de datos se les pregunta por [ISO 27001](#). Quien ya está alcanzado por la Ley 21.663 como OIV o prestador de servicios esenciales tiene armados el proceso de notificación y el sistema de gestión, y puede usarlos como prueba ante clientes de la UE. Si todavía no lo tiene, puede armarlo según ISO 27001 en una plataforma GRC como [Sightadel](#), que también cubre NIS2. Muchos clientes revisan además sus sistemas accesibles desde afuera. Con [veyrisk](#) usted mismo vigila esa superficie de ataque.

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. Con la Ley 21.719 y una autoridad de protección de datos propia, en adelante podrá remitirse a un marco legal más cercano al europeo.

Un punto de partida razonable para empresas chilenas:

1. Verifique si queda alcanzado por la Ley 21.663, como prestador de servicios esenciales o como OIV.

2. Prepárese para la Ley 21.719 como si el 01/12/2026 fuera seguro. Lo que haga para eso lo esperan de todos modos sus clientes de la UE.
3. Unifique en un solo flujo los procesos de notificación ante la ANCI, la nueva Agencia de Protección de Datos y sus clientes de la UE.
4. Para la madera, la celulosa y otros productos del EUDR, revise con su comprador la diligencia debida simplificada.
5. Para el acero, el aluminio y los fertilizantes, aclare qué datos de emisiones necesita su importador para el CBAM.

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

Acuerdo con la UE

Chile está asociado al Mercosur, pero no forma parte del Acuerdo UE-Mercosur. Tiene su propio marco de acuerdos con la UE: el Acuerdo Marco Avanzado y el Acuerdo Comercial Interino, ambos firmados el 13/12/2023. El Acuerdo Comercial Interino está en vigor desde el 01/02/2025 y reemplaza la parte comercial del Acuerdo de Asociación de 2002. Incluye, entre otros, capítulos sobre energía y materias primas y sobre desarrollo sostenible. Para la preferencia arancelaria necesita una declaración de origen.

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. La mayor parte del comercio entre Chile y la UE está libre de aranceles. En los productos elaborados, la regla de origen define si hubo suficiente valor agregado en Chile. Para el litio y el cobre, el acuerdo contiene reglas propias sobre materias primas y energía. Su importador en la UE puede ayudarlo a emitir correctamente la declaración de origen. Conserve las pruebas durante varios años, porque la aduana puede hacer controles posteriores.

Aun con el acuerdo, el EUDR, el CBAM y el RGPD se aplican sin cambios a las mercaderías y servicios chilenos.

FAQ

¿Cuándo entra en vigor la nueva ley de protección de datos en Chile?

La Ley 21.719 entra en vigor el 01/12/2026. El proyecto Boletín 18.623-07 la postergaría al 01/12/2027, pero todavía no ha sido aprobado (al 11/10/2026).

¿En cuánto tiempo hay que notificar un ciberincidente en Chile?

Alerta temprana dentro de las 3 horas al CSIRT Nacional, actualización dentro de las 72 horas (OIV, 24 horas) e informe final dentro de los 15 días desde la alerta temprana.

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

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

¿El cobre chileno está alcanzado por el CBAM?

No. El cobre no figura entre los productos del CBAM. Más información en la página sobre el [CBAM](#).

¿Cómo muestro a un cliente de la UE qué sistemas tengo expuestos en internet?

Con un análisis externo de la superficie de ataque. [veyrisk](#) revisa desde afuera servicios abiertos, certificados, vulnerabilidades y la configuración de DNS y correo, y entrega un informe que puede usar como evidencia. Cómo se ve, lo muestra el [informe de ejemplo](#).

Fuentes · Actualizado: 11 de octubre 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/>

Comisión Europea, DG Comercio: Chile: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/chile_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>