

PAÍS DA UE · BÁLTICOS

Estônia: o que os clientes esperam dos fornecedores

A Estônia é pequena e digital. Quem fornece serviços de TI para lá está sujeito, desde janeiro de 2026, a uma obrigação expressa de notificação da lei estoniana de cibersegurança, mesmo como prestador no exterior.

IDIOMA OFICIAL Estoniano	MAIOR PORTO DE CARGA Muuga (Port of Tallinn)	NIS2 Küberturvalisuse seadus, alterada, desde 01/01/2026	AUTORIDADE DE PROTEÇÃO DE DADOS Andmekaitse Inspektsioon
IVA 24 % alíquota padrão			

A Estônia como mercado para a América do Sul

Como mercado para produtos agrícolas da América do Sul, a Estônia é pequena. Vinho, frutas, café e carne costumam chegar por atacadistas que abastecem vários países bálticos ou também a Finlândia. O país é mais interessante para prestadores de serviços: órgãos públicos e empresas trabalham de forma quase toda digital, e o software muitas vezes é desenvolvido com parceiros no exterior. Uma equipe em Montevidéu ou Córdoba programando para um cliente em Tallinn não chama atenção por lá.

O maior porto de carga é Muuga, cerca de 17 quilômetros a leste de Tallinn. Ele pertence ao Port of Tallinn e tem um terminal de contêineres. A mercadoria da América do Sul em geral chega por um porto de transbordo na Europa Ocidental e segue em navio alimentador para o Báltico.

O que é igual em toda a UE e o que vale no país

Alfândega e regras de produto são iguais em toda a UE. Desde 01/05/2026, a parte comercial do [acordo UE-Mercosul](#) é aplicada provisoriamente. Se a sua mercadoria é colocada em livre prática em Roterdã, depois disso ela também é mercadoria da UE na Estônia. Os detalhes estão no [guia de exportação para a UE](#).

São regulados no nível nacional o idioma das informações ao consumidor (estoniano), o IVA (alíquota padrão de 24 %) e as embalagens. A Estônia mantém um registro de embalagens previsto na lei de

embalagens (pakendiseadus); a obrigação de declarar é de quem coloca mercadoria embalada no mercado estoniano, ou seja, em geral o seu importador. Desde 12/08/2026 vale também o regulamento europeu de embalagens (UE) 2025/40.

NIS2 na Estônia

A Estônia não escreveu uma lei nova: alterou a lei de cibersegurança já existente (Küberturvalisuseadus, KüTS). A alteração foi publicada no Riigi Teataja em 30/12/2025 e vale desde 01/01/2026. As empresas abrangidas tiveram três meses para se registrar pelo portal do Estado eesti.ee. Para a implementação completa das obrigações há um período de transição de três anos; as obrigações de notificação e o registro já valem.

Quase tudo fica a cargo da Autoridade do Sistema de Informação do Estado (Riigi Infosüsteemi Amet, RIA). Ela é órgão de supervisão, ponto de contato central e CSIRT; os incidentes são tratados pela sua equipe CERT-EE. Os prazos seguem a diretiva: primeira notificação em até 24 horas, notificação do incidente em 72 horas.

Ponto importante para fornecedores: pelo § 8, n.º 1¹, da KüTS, um prestador que opera sistemas ou hospeda dados para uma empresa abrangida precisa informar o seu contratante sobre um incidente em até 24 horas. Perante a autoridade, quem responde é o seu cliente, mas ele vai colocar esse prazo no seu contrato.

Os requisitos técnicos estão no decreto governamental n.º 121. Empresas maiores precisam implementar o padrão estoniano de segurança da informação E-ITS ou apresentar à RIA um certificado [ISO 27001](#) válido. Para todas valem medidas mínimas em nove áreas, entre elas, de forma expressa, a gestão de parceiros externos. Na prática, o seu cliente vai avaliar você como parceiro externo. Um relatório do [veyrisk](#) sobre a sua superfície de ataque é uma comprovação que ele consegue ler rápido. Mais sobre a diretiva na página [NIS2](#).

Proteção de dados e cadeia de suprimentos

A autoridade de proteção de dados é a Andmekaitse Inspektsioon, que fiscaliza o [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#) na Estônia. Para prestadores da América do Sul, isso significa na prática: contrato de tratamento de dados, lista de medidas técnicas e organizacionais e, para fluxos de dados ao seu país, cláusulas contratuais-padrão quando não houver decisão de adequação. A UE adotou decisões de adequação para Argentina, Brasil e Uruguai; para esses países, os dados podem fluir sem cláusulas contratuais-padrão. Para Chile, Colômbia, Peru, Equador, Paraguai e Bolívia não há decisão.

A Estônia não tem lei própria de cadeia de suprimentos. As empresas estonianas, em sua maioria, são pequenas demais para a [CSDDD](#); exigências sobre direitos humanos e meio ambiente tendem a chegar até você por grandes grupos escandinavos que comprem nos países bálticos.

O que os clientes estonianos costumam exigir

Em serviços de TI, clientes estonianos perguntam cedo sobre segurança e armazenamento de dados: onde ficam os dados, quem tem acesso, em quanto tempo você notifica um incidente? Um certificado ISO 27001 ajuda em dobro, porque também é reconhecido como comprovação pela lei estoniana. Contratos e questionários costumam ser em inglês.

No varejo de alimentos valem as comprovações usuais, ou seja, um padrão reconhecido pela GFSI como [IFS](#), [BRCGS](#) ou [FSSC 22000](#) e, para café, cacau, soja, carne bovina e madeira, as obrigações de diligência do [EUDR](#).

Como proceder:

1. Verifique se o seu cliente estoniano está sujeito à lei de cibersegurança.
2. Monte um canal de notificação que garanta o repasse de incidentes ao cliente em até 24 horas.
3. Documente suas medidas seguindo as nove áreas das medidas mínimas estonianas.
4. Considere um certificado ISO 27001 se você atende vários clientes na Estônia.

Contatos úteis

ÓRGÃO	PARA QUÊ
Maksu- ja Tolliamet	autoridade tributária e aduaneira da Estônia
Riigi Infosüsteemi Amet (RIA), CERT-EE	Cibersegurança e notificação de incidentes
ProChile, escritório de Estocolmo	responsável também pela Estônia, para exportadores chilenos
Enterprise Europe Network	Busca de parceiros e orientação sobre direito da UE

Não encontramos uma câmara de comércio bilateral entre a Estônia e algum país sul-americano. Pergunte ao setor comercial da sua embaixada qual representação é responsável pela Estônia; muitas vezes ela atende também todos os países bálticos ou os nórdicos.

FAQ

Como prestador da América do Sul, preciso notificar incidentes na Estônia?

Não à autoridade, mas ao seu cliente: em até 24 horas, se você opera sistemas ou hospeda dados para uma empresa abrangida (§ 8, n.º 1¹, da KüTS).

A ISO 27001 substitui o E-ITS?

Sim. O decreto n.º 121 aceita um certificado ISO/IEC 27001 válido, com escopo adequado, como alternativa ao padrão estoniano E-ITS. Isso vale para o seu cliente; para você como fornecedor, é a comprovação mais forte. Para montar o ISMS até a certificação, o [Sightadel](#) conduz pela norma e é hospedado na Alemanha. O certificado em si é emitido por um organismo acreditado.

Qual é o IVA na Estônia?

A alíquota padrão é de 24 %.

Fontes · Atualizado em: 11 de outubro de 2026

Küberturvalisuse seaduse muutmise seadus, RT I, 30.12.2025, 4: <https://www.riigiteataja.ee/akt/130122025004>

RIA: Uuest aastast laienes küberturvalisuse seadus: <https://www.ria.ee/uudised/uuest-aastast-laienes-kuberturvalisuse-seadus>

RIA, CERT-EE: Reporting a cyber incident: <https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/reporting-cyber-incident>

Andmekaitse Inspektsioon: <https://www.aki.ee/>

Comissão Europeia: decisões de adequação: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Comissão Europeia, Your Europe: taxas de IVA: https://europa.eu/youreurope/business/taxation/vat/vat-rules-rates/index_pt.htm

Port of Tallinn: Muuga Harbour: <https://www.ts.ee/en/muuga-harbour/>

Gobierno de Chile: Agregadurías en Suecia (ProChile): <https://www.chile.gob.cl/suecia/agregadurias-civiles>

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>