

REGRA DA UE · CIBERSEGURANÇA

NIS2: a cibersegurança que seus clientes da UE repassam

A NIS2 obriga as empresas da UE a verificar também a segurança dos seus fornecedores. Por isso questionários, cláusulas de notificação e direitos de auditoria chegam até você, mesmo que a lei nem mencione sua empresa.

BASE LEGAL	VALE DESDE	PRAZOS DE NOTIFICAÇÃO	AFETA
Diretiva (UE) 2022/2555	18/10/2024 (leis nacionais)	24 h, 72 h, 1 mês	Fornecedores de TI, software e indústria

Em resumo

A NIS2 é uma diretiva da UE sobre cibersegurança. Ela vale para entidades “essenciais” e “importantes” de 18 setores, entre eles energia, transportes, saúde, infraestrutura digital, gestão de serviços de TIC, alimentos, química e a fabricação de determinados bens, como máquinas, veículos ou eletrônicos. Por ser uma diretiva, cada Estado-Membro aprovou a sua própria lei. As obrigações básicas, porém, são as mesmas em todos eles.

Dois artigos importam para você. O artigo 21 exige uma gestão de riscos de segurança da informação, e isso inclui expressamente a segurança da cadeia de suprimentos (n.º 2, alínea d). A entidade precisa levar em conta as vulnerabilidades de cada fornecedor direto, a qualidade dos seus produtos e as suas práticas de segurança, inclusive o desenvolvimento seguro (n.º 3). O artigo 23 regula a notificação de incidentes significativos às autoridades: alerta precoce em até 24 horas, notificação em até 72 horas e relatório final após um mês.

Uma empresa da UE só consegue cumprir esses prazos se os seus prestadores de serviços também avisarem rápido. Por isso eles aparecem hoje em muitos contratos de fornecimento, muitas vezes ainda mais apertados.

Quem é afetado na América do Sul

A maioria das empresas da região é afetada pela NIS2 de forma indireta. Seu cliente na Alemanha, na Espanha ou nos Países Baixos tem a obrigação e a repassa por contrato. Casos típicos:

- Desenvolvimento nearshore em Buenos Aires, Montevidéu, Medellín ou Lima, criando software para uma distribuidora de energia ou um hospital na UE.

- Suporte de TI e call centers com acesso aos sistemas do cliente.
- Fabricantes de controladores, sensores ou equipamentos industriais, por exemplo de São Paulo ou de Córdoba, que fornecem para empresas de saneamento, fabricantes ou operadores logísticos.
- Processadoras de alimentos cujos compradores estão eles mesmos sujeitos à NIS2 e, por isso, também perguntam pela segurança de TI da produção.

Você é afetado diretamente se oferece determinados serviços digitais na UE: computação em nuvem, data centers, redes de distribuição de conteúdo, serviços gerenciados e serviços gerenciados de segurança, serviços de DNS, registro de domínios, marketplaces online, mecanismos de busca e redes sociais. Pelo artigo 26, esses fornecedores ficam sob a jurisdição do Estado-Membro do estabelecimento principal. Quem não tem estabelecimento na UE, mas presta serviços ali, precisa nomear um representante na UE (art. 26, n.º 3). Sem ele, qualquer Estado-Membro onde os serviços são prestados pode agir (art. 26, n.º 4). Um provedor de serviços gerenciados de Porto Alegre com clientes em Portugal deveria pedir uma análise jurídica disso.

Mesmo sem obrigação direta, vale a pena ler a lei: quase toda cláusula que um cliente da UE apresenta pode ser rastreada até o artigo 21 ou 23. Quem sabe disso negocia com mais facilidade.

Prazos

Os Estados-Membros tinham até 17/10/2024 para transpor a NIS2, e as regras nacionais valem desde 18/10/2024. Vários países atrasaram. Na prática, hoje isso já está resolvido em todos os grandes mercados, e os departamentos de compras trabalham com as novas exigências.

Em janeiro de 2026 a Comissão propôs uma alteração pontual da NIS2, junto com um novo marco jurídico para a segurança das cadeias de suprimentos de TIC. Até a aprovação, a diretiva continua valendo na versão atual. Para fornecedores, tudo indica que o tema da cadeia de suprimentos vai ganhar peso. Quem começa a se estruturar agora quase não terá retrabalho depois, porque as obrigações dos artigos 21 e 23 já valem hoje e são a base de qualquer pedido de cliente. Contratos-quadro renegociados com clientes da UE já trazem essas cláusulas de qualquer forma.

NOTIFICAÇÃO PELO ART. 23	PRAZO PARA A ENTIDADE DA UE	O QUE ISSO SIGNIFICA PARA VOCÊ
Alerta precoce	24 horas a partir do conhecimento	Clientes muitas vezes exigem o seu aviso em poucas horas

NOTIFICAÇÃO PELO ART. 23	PRAZO PARA A ENTIDADE DA UE	O QUE ISSO SIGNIFICA PARA VOCÊ
Notificação do incidente	72 horas	Primeira avaliação, sistemas afetados, indicadores
Relatório final	1 mês	Causa, medidas, efeitos transfronteiriços

O que os clientes da UE pedem na prática

As exigências são muito parecidas entre si. Conte com estes pontos:

- Um questionário de segurança, muitas vezes baseado no Anexo A da ISO/IEC 27001.
- Um certificado [ISO/IEC 27001](#) ou, para fornecedores de SaaS com clientes nos EUA, alternativamente um [relatório SOC 2 Tipo II](#).
- Cláusulas contratuais sobre notificação de incidentes de segurança, muitas vezes em até 24 horas ou menos.
- Direitos de auditoria presencial ou remota.
- Comprovações de gestão de vulnerabilidades e de testes de intrusão.
- No caso de software, uma lista de componentes (SBOM) e informações sobre desenvolvimento seguro.
- Um plano de continuidade de negócios e de recuperação.

Um certificado responde de uma vez a boa parte do questionário. Sem ele, você precisa comprovar cada pergunta separadamente, e de novo para cada cliente.

Cuidado com contradições. Quem informa no questionário que todas as contas usam autenticação de dois fatores e depois, na auditoria, precisa mostrar exceções para sistemas legados perde credibilidade. Melhor responder com franqueza e indicar até quando a lacuna será fechada. Guarde as respostas em um lugar central, para que vendas e TI passem as mesmas informações a cada novo cliente. Uma plataforma GRC como o [Sightadel](#) serve para isso: as respostas ficam ligadas às evidências e podem ser reaproveitadas para a ISO/IEC 27001. Em concorrências de grandes grupos europeus, a avaliação de segurança muitas vezes decide se você chega ou não à lista final.

Primeiros passos

1. Verifique se você oferece na UE algum dos serviços citados no artigo 26. Se sim, busque orientação jurídica sobre o representante na UE.

2. Monte uma lista dos seus clientes da UE e dos setores deles. Um cliente de energia ou saúde vai exigir mais do que um varejista.
3. Defina quem na empresa avalia incidentes de segurança e informa o cliente, com substituto e telefone.
4. Examine seus sistemas principais de fora: quais servidores, acessos e serviços estão acessíveis pela internet? Ferramentas como o [veyrisk](#) mostram isso de forma contínua.
5. Responda com honestidade a um questionário real de um cliente e marque as lacunas. É dali que sai o seu plano de ação.
6. Planeje a certificação ISO/IEC 27001 com antecedência, porque estruturar o sistema de gestão e passar pela auditoria leva tempo.

O [Diagnóstico UE](#) gratuito mostra em dez minutos em que ponto você está.

Relação com certificações

A NIS2 não exige nenhum certificado. Mas os clientes da UE aceitam comprovações reconhecidas, porque com elas documentam a sua própria diligência. A [ISO/IEC 27001](#) cobre a maior parte das perguntas, desde que o organismo de certificação seja acreditado, na região por exemplo pela Cgcre no [Brasil](#), pelo OAA na [Argentina](#) ou pelo ONAC na [Colômbia](#). Fornecedores da indústria automotiva precisam também do [TISAX](#). Se você trabalha para bancos ou seguradoras, entra o [DORA](#), e para produtos conectados, o [Cyber Resilience Act](#).

Olhar para o próprio país também ajuda. O [Chile](#) tem, com a Ley Marco de Ciberseguridad, uma lei parecida com a NIS2 em muitos pontos; no [Uruguai](#) há obrigações de notificação para setores críticos. Quem já está obrigado ali tem parte do trabalho feito.

FAQ

A NIS2 vale para a minha empresa na América do Sul?

Diretamente, só se você oferece na UE determinados serviços digitais, como nuvem, data center, serviços gerenciados ou DNS. Em todos os outros casos, seu cliente da UE repassa as obrigações a você por contrato.

Preciso de um certificado ISO 27001 por causa da NIS2?

Pela lei, não. Muitos clientes da UE exigem mesmo assim, porque ele simplifica a verificação da cadeia de suprimentos prevista no artigo 21. Mais detalhes na página sobre a [ISO/IEC 27001](#).

Com que rapidez preciso notificar um incidente ao meu cliente da UE?

Isso está no seu contrato. Como o próprio cliente precisa emitir um alerta precoce em até 24 horas, muitos contratos exigem o aviso em poucas horas.

O que é um representante na UE?

Uma pessoa ou empresa estabelecida na UE que serve de ponto de contato das autoridades para determinados fornecedores de serviços digitais sem estabelecimento na UE (art. 26, n.º 3).

Qual ferramenta ajuda a comprovar a gestão de vulnerabilidades?

O [veyrisk](#) verifica de fora o que sua empresa expõe na internet, como serviços abertos, certificados e a configuração de DNS e e-mail, e entrega um relatório que você pode apresentar ao cliente da UE. A correção das falhas continua sendo tarefa sua.

Fontes · Atualizado em: 11 de outubro de 2026

Diretiva (UE) 2022/2555 (NIS2), EUR-Lex: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Comissão Europeia: Diretiva NIS2: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

ENISA: Diretiva NIS2: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

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>