DOCUMENTO TÉCNICO

# Rumo à conformidade com a NIS2: como o zero trust precisa ser uma parte essencial dessa jornada

# Índice

1. Resumo executivo: NIS2 e o papel de um modelo zero trust no aumento da resiliência cibernética 3

2. Visão geral da diretiva NIS2 e seu escopo 4

3. A abordagem zero trust da Zscaler é compatível com a diretiva NIS2 5

4. Principais áreas de conformidade com a NIS2 e como a Zscaler pode ajudar 6

- 4.1 Medidas de gerenciamento de riscos de cibersegurança da NIS2 7
- 4.2 Governança e gerenciamento de riscos da NIS2 7
- 4.3 Requisitos de notificação de incidentes da NIS2 8
- 4.4 Supervisão e execução da NIS2 9

# Resumo executivo

## NIS2 e o papel de um modelo zero trust no aprimoramento da resiliência cibernética

A promulgação da diretiva de segurança de redes e informações 2 (NIS2) marca uma evolução significativa no compromisso da União Europeia (UE) de reforçar a cibersegurança em seus estados-membros. A NIS2 substitui a diretiva NIS anterior e expande seu escopo para uma gama mais ampla de setores e subsetores, ao mesmo tempo em que reforça os requisitos de segurança, incluindo tornar a cibersegurança uma prioridade de gerenciamento e governança. Embora a NIS2 tenha entrado em vigor em 2023, a data limite é outubro de 2024, quando os estados-membros da UE devem ter leis nacionais aplicáveis em vigor implementando a NIS2. Como a implementação da NIS2 pode variar ligeiramente em cada estado-membro, este documento técnico se concentra nos requisitos e princípios de alto nível da própria diretiva.

Nenhuma solução ou fornecedor de software por si só pode garantir a conformidade com a NIS2. No entanto, a adesão aos princípios de zero trust (que a própria diretiva sugere que as entidades adotem como uma prática básica de higiene cibernética) aborda uma série de critérios exigidos pela diretiva. Implementar a arquitetura zero trust no ambiente de uma organização, em elementos distribuídos de uma rede e em terceiros de uma organização pode reduzir radicalmente as superfícies de ataque e remover uma série de variáveis técnicas que podem dificultar o progresso em direção à conformidade com a NIS2. O zero trust deve ser o principal veículo usado pelas organizações para aumentar a resiliência; um parceiro sólido que oferece zero trust pode auxiliar nas jornadas de conformidade das organizações.

A jornada rumo à conformidade deve ser estruturada e comunicada a todas as organizações abrangidas pela nova diretiva. Pesquisas recentes da Zscaler com equipes de TI europeias analisaram o estado de prontidão das organizações para a conformidade.

Setenta e um por cento dos líderes de TI entrevistados acreditam que a modernização da segurança exige uma mudança significativa de mentalidade, não apenas um exercício de conformidade.

No entanto, as atitudes mantidas por diferentes partes interessadas que impulsionarão a conformidade variam drasticamente. Embora 80% dos líderes de TI pesquisados estejam confiantes de que suas organizações estarão em conformidade dentro do prazo, apenas 53% acreditam que suas equipes entendem completamente o escopo das obrigações da NIS2. Quando questionados sobre a compreensão da liderança corporativa em relação às obrigações de conformidade, esse número cai para 49%. Mais de 60% dos entrevistados acreditam que a NIS2 exigirá uma mudança significativa em sua estratégia de segurança atual.

A Zscaler está posicionada de forma única para ajudar organizações a navegar pelas mudanças introduzidas pela NIS2, dada nossa experiência em segurança na nuvem. Ao adotar a arquitetura zero trust da Zscaler, organizações de todos os tamanhos podem atender aos principais requisitos da diretiva, aprimorando seus mecanismos de defesa, reduzindo sua exposição a riscos cibernéticos e simplificando as atividades de conformidade. Os princípios do zero trust estão intimamente alinhados com os objetivos da NIS2 ao eliminar sistematicamente direitos de acesso desnecessários, verificar rigorosamente todas as conexões e minimizar o impacto potencial de incidentes de segurança. A Zscaler fornece uma variedade de recursos e ferramentas que dão suporte aos esforços de conformidade com disposições específicas da NIS2, incluindo aplicação de políticas, detecção de incidentes e processos de resposta.

# Visão geral da diretiva NIS2 e seu escopo

A NIS2 entrou em vigor em 2023, com prazo de implementação pelos estados-membros da UE em outubro de 2024. Os formuladores de políticas da UE promulgaram esta nova legislação crítica em resposta à necessidade de a UE aumentar sua resiliência cibernética em uma era de crescentes ataques cibernéticos contra cidadãos, empresas e economias europeias. A NIS2 enfatiza a responsabilidade das entidades em garantir a segurança da rede e dos sistemas de informação, solicitando que tenham uma cultura de governança e estruturas abrangentes de gerenciamento de riscos.  A NIS2 é consistente com uma tendência crescente na UE em direção a uma regulamentação mais direta dos esforços de resiliência cibernética. (Por exemplo, a Lei de Resiliência Operacional Digital (DORA), que entrará em vigor em janeiro de 2025, é uma estrutura separada para gerenciar e mitigar riscos de TIC no setor financeiro.)

A diretiva NIS2 adiciona novos setores industriais, bem como novos tipos de entidades dentro de setores existentes, à diretiva NIS original. Essa expansão responde à crescente percepção de que uma ampla gama de atividades econômicas e sociais são altamente dependentes da infraestrutura de TI, que as ameaças cibernéticas a esses setores estão crescendo e que as interrupções podem ter efeitos em cascata por toda a UE.

Os setores industriais na NIS2 são categorizados como “essenciais” ou “importantes” para refletir sua criticidade ou o serviço que fornecem. Embora os requisitos de cibersegurança e de notificação de incidentes sejam os mesmos para ambos os grupos, as duas categorias de entidades estarão sujeitas a regimes de supervisão e execução ligeiramente diferentes, incluindo o valor de possíveis multas por não conformidade (mais sobre isso abaixo).

> “Com o prazo se aproximando, as organizações enfrentam esforços acelerados de conformidade, potencialmente em detrimento de outros aspectos vitais da cibersegurança. 60% dos participantes da pesquisa expressam receios de que os esforços concentrados na conformidade com a NIS 2 possam resultar na negligência de outras áreas críticas de segurança. Consequentemente, é fundamental que os líderes organizacionais ofereçam suporte substancial aos departamentos de TI, garantindo uma abordagem holística à conformidade que mitigue os riscos de vulnerabilidades e contratempos operacionais.”
>
> **James Tucker,** chefe do programa CISOs in Residence para EMEA na Zscaler

## Setores e subsetores abrangidos pela NIS2[1]

| Entidades essenciais (“setores de alta criticidade”) | |
|---|---|
| **Energia** | Inclui eletricidade, petróleo, gás, aquecimento e refrigeração urbanos e hidrogênio |
| **Transporte** | Inclui transporte aéreo, ferroviário, aquático e rodoviário |
| **Bancos (instituições de crédito)** | |
| **Infraestruturas do mercado financeiro** | |
| **Saúde** | Inclui saúde, produtos farmacêuticos |
| **Água potável** | |
| **Água residual** | |
| **Infraestrutura digital** | Inclui provedores de ponto de troca de internet (IXP), provedores de serviços de DNS, registros de nomes de TLD, provedores de serviços de computação na nuvem, provedores de serviços de data center, provedores de rede de distribuição de conteúdo, provedores de serviços confiáveis, provedores de redes públicas de comunicações eletrônicas e provedores de serviços de comunicações eletrônicas disponíveis ao público |
| **Gerenciamento de serviços de TIC (business-to-business)** | Inclui provedores de serviços gerenciados e provedores de serviços de segurança gerenciados |
| **Administração pública** | Entidades da administração pública de governos centrais e regionais, conforme definidas pelas leis nacionais dos estados-membros |
| **Espaço (operadores de infraestrutura terrestre)** | |
| **Entidades importantes (“outros setores críticos”)** | |
| **Serviços postais e de entrega rápida** | |
| **Gerenciamento de resíduos** | |
| **Fabricação, produção e distribuição de produtos químicos** | |
| **Produção, processamento e distribuição de alimentos** | |
| **Manufatura** | Inclui uma ampla gama de produtos de manufatura, como dispositivos médicos, computadores e eletrônicos, equipamentos elétricos, máquinas e equipamentos, veículos automotores, equipamentos de transporte |
| **Provedores digitais** | Inclui provedores de mercados on-line, provedores de mecanismos de busca on-line e provedores de plataformas de serviços de redes sociais |
| **Organizações de pesquisa** | |

1. Há algumas exceções a essas categorias; consulte os anexos I e II da diretiva para obter mais detalhes. Também são excluídas as entidades da administração pública cujas atividades sejam predominantemente de segurança nacional, segurança pública, defesa ou aplicação da lei. Além disso, a diretiva aplica-se apenas a entidades que se qualificam como “médias empresas” na UE (empresas com mais de 250 pessoas e volume de negócios anual superior a 50 milhões de euros). Ao mesmo tempo, algumas exceções aplicam a NIS2 a algumas entidades menores.

# A abordagem zero trust da Zscaler é compatível com a diretiva NIS2

**A plataforma Zero Trust Exchange™ da Zscaler reduz a complexidade associada à segurança de rede tradicional, facilitando o atendimento aos requisitos da diretiva NIS2 pelas organizações.** A Zero Trust Exchange™ é uma arquitetura nativa da nuvem, baseada em SASE, desenvolvida especificamente para atender às demandas de operações comerciais globais com diversos requisitos tecnológicos e operacionais. Utilizar segmentação granular para compartimentar uma rede, aplicar o acesso de privilégio mínimo para restringir as permissões dos usuários e manter o monitoramento contínuo do tráfego são medidas proativas que ajudam a identificar e responder aos criminosos, minimizando os danos potenciais e o impacto dos ataques.

A Zero Trust Exchange™ também permite que as organizações reduzam sua superfície de ataque, impeçam a movimentação lateral e diminuam os riscos de violação ao abstrair a segurança da infraestrutura de rede. Isso garante que os usuários se conectem com segurança aos aplicativos sem expor as redes à internet, reduzindo significativamente o risco de ataques. Os recursos da plataforma dão suporte aos esforços de conformidade exigidos pelos mandatos da NIS2 para manuseio seguro de dados, controles de acesso e gerenciamento de incidentes.

A plataforma aprimora a segurança protegendo todo o tráfego, usuários e dispositivos, garantindo bloqueio de ameaças em tempo real e inspeção abrangente do tráfego. A Zscaler também melhora a produtividade dos administradores com gerenciamento global unificado e administração de políticas, eliminando a necessidade de manutenção de hardware e permitindo o foco em atividades de valor agregado. A plataforma dda Zscaler aprimora o desempenho da internet para usuários finais e conexões diretas à internet, e nossa conformidade com as principais estruturas de segurança, como ISO 27001 e SOC2 Tipo II, aprimora ainda mais a experiência geral dos usuários e a postura de segurança organizacional. Mais detalhes sobre zero trust e a abordagem da Zscaler para a arquitetura zero trust podem ser encontrados na Zpedia da Zscaler.

## Alinhamento da Zscaler com a NIS2

A abordagem abrangente da Zscaler para segurança e conformidade nos permite reagir rapidamente e nos alinhar às regulamentações existentes, novas e emergentes, como a NIS2. O programa interno de gerenciamento de riscos de cibersegurança da Zscaler garante a adesão a padrões internacionalmente reconhecidos, como ISO 27001 e SOC 2. O alinhamento com esses padrões fundamentais permite que a Zscaler incorpore efetivamente um conjunto diversificado de controles de segurança para identificar, prevenir, detectar, responder e se recuperar de ameaças associadas em nossos produtos e serviços. A Zscaler utiliza uma estrutura de controles comuns que se concentra em competências essenciais de cibersegurança, como o estabelecimento de um programa de gerenciamento de riscos de segurança da informação, práticas seguras da cadeia de suprimentos, gerenciamento de riscos de terceiros, avaliações contínuas de riscos, relatórios de incidentes, divulgação de vulnerabilidades, entre outros. Uma lista atualizada dos padrões de segurança e conformidade que a Zscaler mantém pode ser encontrada na **página de visão geral de conformidade da Zscaler**.

Além disso, a Zscaler mantém o Zscaler Trust **Portal** para fornecer aos clientes insights em tempo real sobre as operações da Zscaler, servindo como o principal fórum de comunicação para **incidentes** e **avisos relacionados à Zscaler**.

# Principais áreas de conformidade com a NIS2 e como a Zscaler pode ajudar

A NIS2 delineia a responsabilidade das entidades para garantir segurança de rede e sistemas de informação, exigindo que tenham uma cultura de governança e estruturas de gerenciamento de risco estabelecidas, abrangentes e bem integradas. Para atingir essas metas, a NIS2 inclui medidas de gerenciamento de riscos de cibersegurança, medidas de governança, requisitos de relatórios de incidentes e supervisão e execução, todos descritos abaixo.

Na pesquisa com líderes europeus de TI mencionada acima, 56% dos entrevistados disseram à Zscaler que suas equipes sentem falta de suporte da liderança para cumprir o prazo de conformidade da NIS2. Para auxiliar em suas jornadas de conformidade, os líderes de TI pesquisados disseram que as mudanças mais significativas necessárias em suas organizações foram as seguintes:

- Atualização de pilhas de tecnologia e soluções de cibersegurança: 34%
- Instruir funcionários: 20%
- Instruir líderes: 17%

## Medidas de gerenciamento de riscos de cibersegurança da NIS2

As entidades abrangidas pela diretiva devem adotar medidas técnicas, operacionais e organizacionais proativas para gerenciar os riscos à segurança das redes e dos sistemas de informação que essas entidades utilizam para suas operações ou para a prestação de seus serviços, e para prevenir ou minimizar o impacto de incidentes nos destinatários de seus serviços e em outros serviços que as organizações possam fornecer.

O artigo 21 da diretiva lista as medidas mínimas de gerenciamento de riscos de cibersegurança que as organizações devem tomar, enquanto os considerandos 78 e 89 fornecem mais informações sobre o que os autores da lei esperam.

- **O artigo 21 (medidas mínimas de gerenciamento de riscos de cibersegurança)** especifica que as entidades devem implementar políticas sobre análise de riscos e segurança de sistemas de informação; continuidade de negócios e gerenciamento de crises; segurança da cadeia de abastecimento, incluindo procedimentos de desenvolvimento de qualidade e segurança de produtos e práticas de cibersegurança dos seus fornecedores e prestadores de serviços; práticas básicas de higiene cibernética e formação em cibersegurança; políticas e procedimentos relativos à utilização de criptografia; segurança de recursos humanos, políticas de controle de acesso e gerenciamento de ativos; e uso de soluções de autenticação multifator ou autenticação contínua.
- **De acordo com o considerando 78**, as medidas de gerenciamento de riscos de cibersegurança implementadas pelas entidades abrangidas pela diretiva devem levar em conta o grau de dependência da entidade em relação às redes e aos sistemas de informação; identificar quaisquer riscos de incidentes; prevenir, detectar, responder e recuperar de incidentes e mitigar o seu impacto; abranger dados armazenados, transmitidos e processados; e prever uma análise sistêmica, levando em conta o fator humano.
- **O considerando 89** insta as entidades a implementarem uma série de práticas básicas de higiene cibernética recomendadas, nomeadamente, princípios de zero trust, atualizações de software, configuração de dispositivos, segmentação de rede, gerenciamento de identidade e acesso ou sensibilização de usuários, e formação de pessoal e sensibilização sobre ameaças cibernéticas, phishing ou técnicas de engenharia social. O considerando 89 também insta as entidades a adotarem tecnologias que aprimorem a cibersegurança, como sistemas de inteligência artificial (IA) ou de aprendizado de máquina (ML), para melhorar as suas capacidades e a segurança das redes e dos sistemas de informação.

**Como a Zscaler pode ajudar:** abaixo, descrevemos de forma geral como a Zscaler pode ajudar as entidades a se alinharem a aspectos específicos dessas disposições. Para um mapeamento detalhado das soluções e ferramentas específicas da Zscaler compatíveis com essas disposições, entre em contato com seu representante local da Zscaler. Conteúdo geral e documentos técnicos sobre as soluções da Zscaler podem ser encontrados em https://www.zscaler.com/resources?type=white-papers.

## Governança e gerenciamento de riscos da NIS2

A NIS2 atribui a responsabilidade final à liderança da empresa. A gerência deve aprovar e supervisionar a implementação das medidas de gerenciamento de riscos de cibersegurança da entidade. A gerência também deve seguir o treinamento em cibersegurança e oferecer treinamento semelhante aos seus funcionários regularmente, para que eles adquiram conhecimento e habilidades suficientes para identificar riscos e avaliar as práticas de gerenciamento de riscos de cibersegurança e seu impacto nos serviços da entidade.

**Como a Zscaler pode ajudar:** a Zscaler fornece recursos de segurança abrangentes em seu conjunto de serviços, projetados para ajudar organizações a minimizar sua superfície de ataque e garantir a eficácia dos controles de segurança aplicados em todo o programa de governança e gerenciamento de riscos do cliente.

Zscaler Resilience™ é um conjunto completo de recursos que garante a continuidade ininterrupta dos negócios durante interrupções totais, parciais ou eventos catastróficos imprevisíveis.

O Zscaler Internet Access (ZIA) e o Zscaler Private Access (ZPA) reforçam os fluxos de tráfego e fornecem logs de eventos e transações de segurança para correlação e gerenciamento, permitindo que as organizações monitorem e mitiguem ameaças potenciais de forma eficaz.

A Zero Trust Exchange™ da Zscaler garante que os usuários não sejam inseridos na rede e os aplicativos nunca sejam expostos à internet, reduzindo significativamente a superfície de ataque. A solução também permite que as organizações criem e apliquem políticas sobre os sites de IA generativa com os quais os usuários podem interagir para garantir a proteção de dados sigilosos.

Os recursos de inspeção de SSL da Zscaler aumentam ainda mais a segurança ao descriptografar o tráfego HTTPS para detectar e bloquear conteúdo malicioso.

Os sistemas Risk360™ e Zscaler Posture Control (ZPC) da Zscaler oferecem monitoramento contínuo e detecção de vulnerabilidades, permitindo que as organizações abordem proativamente os riscos de segurança.

A Zscaler Digital Experience (ZDX) fornece rastreamento de inventário de dispositivos, garantindo que os componentes de serviço sejam identificados adequadamente e desativados com segurança quando necessário, contribuindo para minimizar a superfície de ataque.

O Nanolog Streaming Service (NSS) da Zscaler facilita a comunicação perfeita entre a nuvem da Zscaler e os dispositivos de soluções de segurança de terceiros, permitindo o streaming de logs em tempo real para os sistemas de SIEM dos clientes por meio de opções baseadas em VM ou NSS na nuvem.

O Zscaler Cloud Intrusion Prevention Service (IPS), integrado com tecnologias como firewalls e sandboxes, fornece proteção abrangente contra ameaças contra vários ataques, aproveitando assinaturas personalizadas e líderes do setor para monitoramento em tempo real e aplicação de políticas. Além disso, as organizações podem identificar e corrigir vulnerabilidades proativamente usando os recursos da Zscaler, como as políticas de proteção contra ameaças avançadas e proteção contra malware móvel do ZIA, enquanto o Risk360 oferece insights sobre a superfície de ataque externa e o risco de propagação lateral, oferecendo decisões bem fundamentadas para aprimorar a postura de segurança de uma organização e reduzir seu tempo médio de resposta (MTTR).

Por fim, todos os clientes podem se registrar para usar o portal de confiança da Zscaler para relatar incidentes ou suspeitas de incidentes.

## Requisitos de notificação de incidentes da NIS2

As entidades devem notificar as autoridades sobre qualquer incidente que tenha impacto significativo na prestação dos seus serviços. Quando apropriado, as entidades também devem notificar os destinatários dos seus serviços sobre incidentes relevantes que possam afetar negativamente a prestação dos serviços. A NIS2 define um incidente relevante como aquele que causou ou é capaz de causar grave interrupção operacional dos serviços ou perda financeira para a entidade em questão, ou afetou ou é capaz de afetar outras pessoas físicas ou jurídicas, causando danos materiais ou imateriais consideráveis.

O cronograma de notificação de incidentes é o seguinte:

- Um "alerta precoce" dentro de 24 horas após tomar conhecimento do incidente relevante;
- Uma notificação formal de incidente dentro de 72 horas após tomar conhecimento do incidente relevante, fornecendo uma avaliação inicial do incidente, incluindo sua gravidade e impacto, bem como (quando disponíveis) indicadores de comprometimento;
- Um relatório final dentro de um mês detalhando o incidente, incluindo sua gravidade e impacto; o tipo de ameaça ou causa-raiz que provavelmente desencadeou o incidente; medidas de mitigação aplicadas e em andamento; e (quando aplicável) impactos transfronteiriços.
- Durante esse processo, as autoridades podem solicitar um relatório intermediário sobre atualizações de status relevantes.

**Como a Zscaler pode ajudar:** as soluções de segurança baseadas na nuvem da Zscaler oferecem recursos de detecção e mitigação de ameaças em tempo real, garantindo que as organizações possam identificar e mitigar ameaças rapidamente. Além disso, ao minimizar as defesas tradicionais baseadas em perímetro em favor da verificação e autorização contínuas de identidade, a arquitetura zero trust da Zscaler ajuda a prevenir movimentações laterais que poderiam agravar a gravidade em caso de violação. Ao avaliar cada solicitação de acesso com base na identidade, autorização e contexto, todo o ambiente fica mais protegido contra incidentes cibernéticos.

## Supervisão e execução da NIS2 (artigos 32 e 33)

Os estados-membros da UE podem usar poderes de supervisão e execução sobre entidades que violem as medidas de gerenciamento de riscos de cibersegurança e as obrigações de relatórios da NIS2. Os regimes de supervisão e execução para entidades essenciais e importantes são ligeiramente diferenciados: para entidades essenciais, a supervisão é ex-ante, enquanto para entidades importantes é ex post (quando há evidências, indicações ou informações de que uma entidade não está em conformidade com a NIS2).
Em geral, as autoridades podem sujeitar entidades abrangidas de qualquer categoria a:

- Inspeções no local e supervisão externa
- Auditorias de segurança direcionadas realizadas por um órgão independente ou por uma autoridade competente
- Verificações de segurança
- Pedidos de informação necessários para avaliar as medidas de gerenciamento de riscos de cibersegurança adotadas, incluindo políticas de cibersegurança documentadas
- Pedidos de acesso a dados, documentos e informações necessárias à supervisão
- Pedidos de provas de implementação de políticas de cibersegurança

A NIS2 também declara que a gerência pode ser responsabilizada pessoalmente por infrações da NIS2, incluindo possíveis proibições temporárias de ocupar cargos de gerência e, como último recurso, as autoridades têm o poder de suspender temporariamente uma certificação ou autorização relacionada aos serviços relevantes prestados ou atividades realizadas pela entidade.

Os estados-membros da UE também podem aplicar multas administrativas por casos de não conformidade com a NIS. Para entidades essenciais, as multas administrativas podem chegar a € 10 milhões ou 2% do faturamento anual total mundial no exercício financeiro anterior, o que for maior. Para entidades importantes, as multas podem chegar a € 7 milhões ou 1,4 % do faturamento anual total mundial no exercício financeiro anterior, o que for maior.

**Como a Zscaler pode ajudar:** a Zscaler oferece suporte às organizações na preparação e resposta a auditorias e escrutínio regulatório por meio de registro abrangente, aplicação consistente de políticas e relatórios detalhados.

Para mais informações sobre a NIS2 e os recursos da Zscaler, entre em contato com seu representante local da Zscaler.





**Sobre a Zscaler**
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.



+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com/br