APRESENTANDO O NIS 2

O que é a Diretiva SRI 2?

Uma diretiva europeia

A Diretiva SRI 2 (Segurança das Redes e da Informação 2) foi adotada em 14 de dezembro de 2022 e publicada no Jornal Oficial da UE em 27 de dezembro de 2022 ao abrigo da Diretiva (UE) 2022/2555 de referência.
Ao contrário de um regulamento da UE, que se aplica direta e uniformemente em todos os Estados-Membros a partir da sua entrada em vigor, uma diretiva da UE estabelece objetivos a alcançar, mas deixa a escolha dos meios aos Estados-Membros e exige a transposição para o direito nacional.

Transposição para o direito nacional

Os Estados-Membros devem ter transposto a SRI 2 até 17 de outubro de 2024, o mais tardar, para aplicação em 18 de outubro de 2024. Alguns Estados ficaram para trás, sem que isso pusesse em causa a emergência de um quadro europeu harmonizado. Em França, é a ANSSI que gere a transposição da diretiva para o direito nacional e assegura a sua aplicação.

Para ir mais longe:

- Diretiva (UE) 2022/2555: https://eurlex.europa.eu/eli/dir/2022/2555/
- Projeto de lei sobre a resiliência das infraestruturas críticas e o reforço da cibersegurança (PRMD2412608L): https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/

Quais são os objetivos do NIS 2?

Na continuidade do NIS 1

A primeira Diretiva SRI visava proteger os principais agentes económicos da União Europeia. Esta nova diretiva alarga o âmbito das entidades em causa, visando 18 setores de atividade. Introduz requisitos mais adequados, em especial no que diz respeito às ciberameaças.

Aprimoramento sem precedentes da segurança cibernética

A NIS 2 fortalece a segurança cibernética na União Europeia, padroniza as regras entre os países e aumenta o nível geral de proteção contra o aumento dos ataques cibernéticos. A diretiva visa as autoridades locais, a segurança das cadeias de abastecimento industriais e a proteção das infraestruturas críticas europeias. Refere-se em grande parte à metodologia da norma ISO/IEC 27001.

Foco em Cibersegurança de Equipamentos Industriais

Em particular, esta diretiva fornece uma estrutura para as chamadas infraestruturas "industriais", ou seja, com elementos OT (Tecnologia Operacional), ICS (Sistemas de Controle Industrial) e IoT (Internet das Coisas). De fato, a segurança cibernética de máquinas e objetos conectados tem sido negligenciada há muito tempo e representa uma vulnerabilidade significativa que é mal dominada pela maioria das organizações. Por exemplo, um CLP usado em uma linha de produção pode ser exposto se a rede não for segmentada. O NIS2 exige que essa exposição seja avaliada e documentada. O NIS 2, portanto, coloca a segurança cibernética industrial de volta no centro das preocupações, principalmente referindo-se ao padrão IEC / ISA 62443.

Em suma

Tema	NIS1 (2016)	NIS2 (2022)
Perímetro	Principais jogadores	18 setores, incluindo PME e autoridades locais
Governança	Menos restritivo	Envolvimento obrigatório da gerência
Sanções	Limitado	Até € 10 milhões ou 2% do faturamento mundial
OT/IoT	Pouco discutido	Central com IEC/ISA 62443

Para ir mais longe

- Diretiva (UE) 2016/1148 (SRI 1) : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
- Tabela de equivalência de conformidade publicada pela ENISA (NIS 2 / ISO 27001 / NIST etc.): https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA_Technical_Implementation_Guidance_Mapping_table_version_1.2.xlsx

O que está mudando com o NIS 2?

Uma abordagem sistêmica para segurança cibernética

A grande novidade do NIS 2 é a abordagem sistêmica da segurança cibernética. Inspirado nas normas ISO/IEC 27001 e IEC/ISA 62443, o NIS 2 exige que as entidades implementem uma estrutura de gerenciamento de riscos semelhante a um Sistema de Gerenciamento de Segurança da Informação (SGSI). Essa estrutura requer gerenciamento de risco sistemático, integrado, avaliado periodicamente e atualizado, envolvendo partes interessadas internas e externas.

Gestão de fornecedores

A gestão de fornecedores está se tornando uma questão fundamental porque a cadeia de suprimentos é um importante vetor de vulnerabilidade. Por exemplo, hardware eletrônico comprometido introduz vulnerabilidades no produto montado pelo fabricante. A NIS 2, portanto, coloca uma ênfase particular no gerenciamento de riscos da cadeia de suprimentos e requer uma avaliação de risco, requisitos contratuais cibernéticos, bem como um processo formalizado de monitoramento e auditoria.

Outros temas

Vários outros temas são tratados especificamente: gerenciamento de incidentes, gerenciamento de crises, continuidade de negócios, treinamento e conscientização de funcionários, controle de acesso, criptografia, etc. A NIS 2 revoluciona assim a gestão de riscos cibernéticos e exige que todas as partes interessadas colaborem para fortalecer a resiliência cibernética coletiva.

Para ir mais longe

- Regulamento de Execução (UE) 2024-2690 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L_202402690
- Guia ENISA de Boas Práticas em https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf da Cadeia de Suprimentos

Quem é afetado pelo NIS 2?

Dois tipos de entidades

A SRI 2 diz respeito às autoridades locais, administrações públicas, PME e grandes empresas. Ele distingue entre duas categorias de entidades:

- **Entidades essenciais** : Pelo menos 250 trabalhadores ou um volume de negócios anual superior a 50 milhões de euros e um balanço anual superior a 43 milhões de euros,

- **Entidades significativas** : que não sejam entidades essenciais e que empreguem pelo menos 50 trabalhadores ou tenham um volume de negócios e um balanço anual superior a 10 milhões de euros.

Dois tipos de setores

Ao mesmo tempo, o NIS 2 identifica 18 setores segmentados em duas categorias:

- **Setores altamente críticos** : Administrações públicas, Água potável, Águas residuais, Energia, Espaço, Gestão de serviços, Tecnologias de informação e comunicação (business-to-business), Infraestruturas do mercado financeiro, Infraestruturas digitais, Saúde, Banca, Transportes,

- **Outros setores críticos** : Fabricação, produção e distribuição de produtos químicos, Fornecedores digitais, Gestão de resíduos, Manufatura, Produção,

processamento e distribuição de alimentos, Pesquisa, Serviços postais e de remessa.

Critérios de aplicabilidade

Assim, uma entidade que atenda aos seguintes critérios provavelmente será afetada pelo NIS 2:

- Mais de 50 funcionários,
- Mais de 10 milhões de euros de volume de negócios,
- Trabalhando em um dos 18 setores cobertos pelo NIS 2.

Para ir mais longe

- Teste de aplicabilidade ANSSI: https://monespacenis2.cyber.gouv.fr/simulateur

Quais são as principais obrigações das organizações industriais?

Vejamos alguns dos requisitos do NIS 2 que, embora não sejam exaustivos, dão uma indicação do nível de gerenciamento de risco necessário.

Governança

- Nomeação de um gerente de segurança cibernética (CISO ou equivalente).
- Envolvimento obrigatório da direção geral na validação das apólices.
- Estabelecimento de uma estrutura de gerenciamento de risco semelhante ao SGSI, conforme definido pela ISO/IEC 27001.

Gestão de Riscos

- Inventário de ativos (OT e IoT), mapeamento de rede.
- Segmentação: separação de TI/OT, particionamento de áreas sensíveis.
- Gerenciamento de patches adaptado a ambientes industriais.

Gestão da cadeia de suprimentos

- Política de Segurança da Cadeia de Suprimentos (PSCA).
- Inclusão de cláusulas de segurança cibernética nos contratos.
- Avaliação contínua e auditorias de fornecedores críticos.

Detecção e notificação de incidentes

- Obrigação de notificar qualquer incidente grave dentro de 24 horas (notificação preliminar).
- Notificação detalhada do incidente em 72 horas.
- Relatório final esperado dentro de 1 mês.

Para ir mais longe

- Guide méthodologique d'application de NIS 2 de l'ENISA : https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Quais são as penalidades previstas pelo NIS 2?

Em caso de incumprimento, as sanções previstas são substanciais:

Sanções para entidades essenciais

Para entidades essenciais: multas de até **€ 10 milhões ou 2%** do faturamento mundial anual (o que for maior).

Sanções para entidades significativas

Para grandes entidades: multas de até **€ 7 milhões ou 1,4%** do faturamento mundial anual (o que for maior).

Responsabilidade dos diretores

Responsabilidade pessoal dos Conselheiros: Uma grande novidade é que os conselheiros e executivos podem ser sancionados diretamente (proibição de exercer, responsabilidade civil ou criminal). Essa disposição eleva a segurança cibernética à categoria de uma questão estratégica para os conselhos de administração.

Como se preparar para a aplicação do NIS 2?

Para se preparar para o NIS 2, recomendamos abordar o projeto como uma transformação técnica, organizacional e gerencial:

1. Formação e informação

Compreender o texto e suas implicações é essencial. A ANSSI recomenda consultar a documentação oficial, seguir o treinamento direcionado e conscientizar a gerência e as equipes-chave.

2. Analise como o NIS 2 afetará você

Você está dentro do escopo de aplicabilidade? Você é fornecedor de entidades essenciais ou importantes que lhe imporão requisitos de segurança cibernética? Se você for elegível para o NIS 2, deverá se registrar no ANSSI.

3. Designe um piloto

Nomeie um gerente de projeto NIS2. Essa pessoa (CISO, CIO, diretor de compliance, etc.) coordena o processo, lidera a governança e garante que as medidas implementadas sejam documentadas.

4. Avalie seu nível de maturidade

Realize um diagnóstico inicial de sua postura de segurança cibernética. Esse inventário deve abranger: mapeamento de ativos (incluindo OT/IoT), gerenciamento de acesso, recursos de detecção e resposta e governança.

5. Crie um plano de ação

Com base nesse diagnóstico, defina um roadmap priorizado, incluindo medidas técnicas (segmentação, gerenciamento de patches, detecção de incidentes), medidas organizacionais (sistema de gestão, procedimentos de notificação, continuidade de negócios) e medidas contratuais (cláusulas com fornecedores).

6. S'organiser pour la notification d'incidents

Construa o seu procedimento de deteção-resposta e notificação (pré-alerta, notificação, relatório final) tendo em conta os prazos impostos pela diretiva. Isso é algo que requer exercícios práticos e evidências documentadas.

7. Implemente ações de segurança

Priorize ações de alto impacto, como redução da superfície de ataque, controle de acesso, SLAs e cláusulas de fornecedores. Meça sua maturidade com KPIs simples (MTTD/MTTR, taxa de patch). Mantenha um "registro de conformidade": essa evidência reduz o risco regulatório e torna o esforço operacional gerenciável.

Para ir mais longe

- Guia ANSSI sobre mapeamento do sistema de informação: https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation
- Guia ANSSI sobre o desenvolvimento de painéis de segurança de sistemas de informação: https://cyber.gouv.fr/publications/tdbssi-guide-delaboration-de-tableaux-de-bord-de-securite-des-systemes-dinformation

Lista de verificação operacional de OT/IoT (10 ações-chave)

1. Mapeie seus ativos de OT/IoT.
2. Identifique seus serviços críticos.
3. Designe um gerente de segurança cibernética.
4. Defina uma política de segurança aprovada pela gerência.
5. Implemente a segmentação de rede OT/IT.
6. Fortaleça a autenticação e o gerenciamento de acesso.
7. Implante ferramentas de detecção de incidentes de OT.
8. Formalize um procedimento de notificação de incidentes.
9. Crie segurança em seus contratos de fornecedores.
10. Treine suas equipes operacionais.

Como a AKENATECH o apoia?

A Akenatech oferece suporte em todas as etapas de sua conformidade com o NIS 2:

Advogado

Governança, gestão de riscos, auditoria de conformidade cibernética, preparação para certificação.

Integração

Implantação de soluções de segurança cibernética adaptadas a ambientes industriais: hardening, segmentação, air-gap, proteção de endpoints, etc.

Serviços gerenciados

CISOs de compartilhamento de tempo, monitoramento regulatório e segurança contínua.

Com sede em Lyon, operamos em toda a França e internacionalmente.

Perguntas Freqüentes

Quem deve cumprir o NIS 2?

Todas as entidades essenciais e importantes enumeradas nos anexos da diretiva (por exemplo, energia, saúde, transportes, agroalimentar).

Quais são os prazos para notificar um incidente?

Notificação inicial em 24 horas, relatório provisório em 72 horas, relatório final em 1 mês.

O NIS 2 se aplica a pequenas e médias empresas?

Apenas as entidades que excedam determinados limiares (50 trabalhadores / 10 milhões de euros de volume de negócios) estão em causa, com exceções para setores críticos.

Qual é a diferença entre NIS1 e NIS 2?

O NIS 2 expande setores, aumenta as obrigações de governança e fortalece as sanções.

Para ir mais longe

- FAQ de la Commission Européenne sur la Directive NIS 2 : https://digital-strategy.ec.europa.eu/fr/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Conclusão

A conformidade com o NIS 2 é obrigatória desde outubro de 2024 para muitas organizações industriais. Esta não é uma formalidade administrativa, mas uma transformação profunda da governança OT/IoT.

A Akenatech ajuda você a passar da teoria à prática com nossos especialistas, ferramentas de segurança e serviços gerenciados.

👉 Entre em contato conosco para um inventário hoje.