



Navigating NIS 2: Ensuring Cybersecurity Compliance in the Digital Era

01

O CONTEXTO REGULATÓRIO E A NIS 2

O contexto da NIS 2

Criar um ambiente propício a uma economia digital segura

Aumentar o nível de ciber-resiliência dos Estados, das empresas e entidades públicas

Melhorar a capacidade de resposta a incidentes no domínio da Cibersegurança

Melhorar a proteção de infraestruturas críticas

ESTRATÉGIA DE CIBERSEGURANÇA DA UE PARA A DÉCADA DIGITAL



Reforço da legislação aplicável



Diretiva NIS 2

Alargamento do âmbito subjetivo, tanto nos setores selecionados como na dimensão das empresas incluídas

Permite a cada país fazer uma seleção adicional

Garantir que as entidades críticas são capazes de prevenir, resistir, absorver e recuperar de incidentes perturbadores

Diretiva quanto à resiliência de infraestruturas críticas



Regulamento DORA (Digital Operational Resilience Act)

Regulamento relativo à **resiliência operacional digital** no setor financeiro, mas que também se aplicará ao setor segurador

Regulamento relativo aos requisitos de cibersegurança para produtos com elementos digitais, que reforça as regras de cibersegurança para garantir produtos de *hardware* e *software* mais seguros.

Regulamento da Ciber-resiliência (EU Cyber Resilience Act)



Estratégia Europeia para a Cibersegurança

Diretiva NIS 2



Principais alterações



ALARGAMENTO

Mais setores vão ser incluídos – como o hidrogénio, farmacêuticas, fornecedores de *data centres*, entre outros



OPERADORES DE SERVIÇOS DIGITAIS

Eliminação da distinção entre operadores de serviços essenciais e de serviços digitais, distinguindo apenas entre operadores de serviços essenciais e entidades importantes



MAIS REQUISITOS DE SEGURANÇA

Estabelece-se uma **lista mínima de requisitos de cibersegurança** que devem ser cumpridos, tendo em conta o risco existente



CADEIAS DE ABASTECIMENTO

Maior proteção para as cadeias de abastecimento e para a relação com fornecedores



SUPERVISÃO

As **regras de supervisão são mais estritas**, harmonizando também as sanções aplicáveis

Âmbito de aplicação

Operadores de serviços essenciais

Infraestruturas do mercado financeiro

Transporte
Transporte aéreo,
ferroviário, aquático e
vias navegáveis interiores
e rodoviário

Bancário

Energia

Eletricidade, petróleo,
gás, **hidrogénio,**
aquecimento e
arrefecimento de
cidades

Infraestruturas digitais

Pontos de troca de tráfego, prestadores de serviços de DNS
e registos de nomes de domínio de topo, **prestadores de**
cloud, prestadores de distribuição de conteúdos, centros
de dados, prestadores de serviços de confiança e
prestadores de comunicações eletrónicas

Saúde

Instalações de prestação
de cuidados de saúde,
laboratórios de
referência,
farmacêuticas e
produtores de
dispositivos médicos

Tratamento de águas residuais

Administração Pública

Espaço

Fornecimento e distribuição
de água potável

Entidades importantes

Serviços postais

Gestão de resíduos

Manufatura, produção
e distribuição de químicos

Produção, processamento
e distribuição de comida
Indústria transformadora

Operadores digitais de
marketplaces, motores de
pesquisa e plataformas
sociais

Organismos de
investigação

Gestão de riscos

As organizações devem adotar uma **abordagem proativa** no que diz respeito à gestão dos riscos de cibersegurança, que inclua a adoção de **políticas de segurança da informação**.

As organizações deverão ainda implementar **medidas de cibersegurança**, designadamente nos seguintes domínios:



Prevenção, deteção e resposta a incidentes

- ✓ Criação de um **quadro sólido de gestão e notificação de incidentes**, testado regularmente e comunicado a todas as partes interessadas
- ✓ Implementação de **procedimentos** tendo em vista a **prevenção, investigação e mitigação** de incidentes



Continuidade do negócio e gestão de crises

- ✓ Garantia da **continuidade do negócio** caso ocorra um incidente de cibersegurança
- ✓ Implementação de um **quadro de resiliência abrangente** de forma a minimizar os danos ocorridos



Segurança da cadeia de abastecimento

- ✓ Participação na **gestão dos riscos associados a terceiros**, podendo justificar-se a implementação de um **quadro de resiliência abrangente da cadeia de abastecimento**

Responsabilidade da administração

Cadeia de abastecimento

- As entidades essenciais e importantes devem, em toda a **cadeia de produção e abastecimento** de produtos e serviços, **mapear e gerir** adequadamente os **riscos de cibersegurança** associados à utilização destes produtos e serviços
- São então encorajadas a incorporar **medidas de gestão dos riscos de cibersegurança** nos **contratos** celebrados e a exercer uma **maior diligência na seleção** dos seus fornecedores e prestadores de serviços diretos



Ao considerar se as políticas de segurança da cadeia de abastecimento dos produtos e serviços de TIC são adequadas, as entidades essenciais e importantes deverão ter em conta:

- ✓ As **vulnerabilidades** de cada **fornecedor e prestador de serviços** direto;
- ✓ A **qualidade geral dos produtos e serviços** e as **medidas de cibersegurança implementadas** pelos seus fornecedores e prestadores de serviços



Sanções



Supervisão

Prestadores de serviços essenciais:

Autoridades podem realizar inspeções aleatórias, auditorias regulares e ad hoc e análises de segurança para verificar vulnerabilidades, bem como solicitar determinadas informações e provas de conformidade

Entidades importantes:

Estão sujeitas a uma supervisão mais ligeira, *ex post*, em caso de provas ou indícios de incumprimento



Sanções e coimas

As autoridades competentes têm poderes para ordenar:

- A cessação de condutas que infrinjam as obrigações legais
- A informação aos titulares afetados por um incidente
- A divulgação pública os aspetos das infrações

As **infrações graves** podem dar origem à aplicação de coimas de, pelo menos, 10 000 000 euros ou 2% do volume de negócios anual total a nível mundial, consoante o montante mais elevado

02

Impacto

Para fazer face à complexa teia regulatória



CAPACITAÇÃO



- É necessário monitorizar e acompanhar todos os desenvolvimentos regulatórios e tecnológicos
- Capacitar os *stakeholders* internos
- E planear e implementar as mudanças necessárias, a nível estratégico, jurídico e tecnológico

Contactos



Obrigada!

Inês Antas de Barros

Sócia da Área de Comunicações,
Proteção de dados e Tecnologia



iab@vda.pt



T. 21 311 3400



www.vda.pt