Cibersegurança

Diretiva NIS 2 & DL 125/2025

ANTAS
DA CUNHA
ECIJA

Principais obrigações Diretiva NIS 2

Antecedentes

Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação na União

(Diretiva NIS)

Lei n.º 46/2018, de 13 de agosto, que transpõe a mesma Diretiva NIS (2016/1148/UE) para o ordenamento jurídico português

(Lei NIS)

Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta a aplicação da Lei n.º 46/2018

(Regulamento NIS)

Atualidade

DIRETIVA (UE) 2022/2555 DO PARLAMENTO EUROPEU E DO CONSELHO de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União

(Diretiva NIS2)

Transposição:
DL 125/2025 de 4 de dezembro

Entidades obrigadas

01
Entidades essenciais

02
Entidades importantes

Classificação de acordo com o grau de criticidade do setor, o tipo de serviço que prestam ou a sua dimensão.

Os Estados-Membros devem elaborar uma lista das entidades consideradas essenciais e importantes.

- Matriz de classificação já publicada pelo CNCS

Setores afetados

- Energia
- Transporte
- Banca e mercados financeiros
- Seguros
- Saúde, laboratórios, investigação
- Água potável, gestão de resíduos
- Infraestrutura digital
- Serviços de gestão de TIC
- Espaço
- Administração Pública
- Bancos Centrais
- Fabrico, produção e distribuição de produtos químicos
- Serviços postais
- Alimentos: produção, distribuição e transformação
- Fabrico de veículos e material de transporte
- Fabrico de produtos sanitários. Fabrico de produtos informáticos, óticos ou elétricos
- Fornecedores de serviços digitais

Em primeiro lugar, afeta as empresas com:

+50 empregados >10 milhões de faturação

Requisitos de segurança mais rigorosos

- Medidas de segurança proporcionais aos riscos a que a organização se encontra exposta

- Os Estados-Membros assegurarão que as organizações apliquem medidas técnicas e organizativas nos seguintes domínios:

Políticas e procedimentos para avaliar a eficácia da gestão dos riscos de cibersegurança.

Segurança na aquisição, desenvolvimento e manutenção de redes e sistemas de informação (incluindo gestão e divulgação de vulnerabilidades).

Implementação e utilização de soluções de autenticação multi-fator, comunicações seguras e sistemas seguros para comunicações de emergência.

Políticas de segurança dos sistemas de informação e análise de riscos.

Políticas e procedimentos de encriptação.

Segurança dos recursos humanos, controlo de acesso e gestão de ativos.

Gestão de incidentes de segurança.

Continuidade das atividades da organização, desde a gestão de cópias de segurança até à recuperação de desastres e à gestão de crises.

Formação obrigatória de cibersegurança para os quadros superiores.

Securitização e externalização da cadeia de abastecimento.

GAP ANALYSIS

01 Análise e gestão dos riscos

- Confidencialidade – Integridade - Disponibilidade
- Processos de negócio
- Infraestruturas dependentes
- Probabilidade e impacto da concretização de uma ameaça
- Nível aceitável de risco motivado
- Abordagem dos riscos inaceitáveis

02 Controlos - medidas de segurança em função dos riscos

- Políticas e procedimentos de segurança da informação
- Organização da segurança da informação (responsabilidades)
- Segurança dos recursos humanos (responsabilidades)
- Gestão de ativos
- Criptografia
- Segurança física
- Segurança operacional e rastreabilidade
- Segurança das comunicações
- Aquisição, desenvolvimento e manutenção de sistemas
- Continuidade das atividades de negócio
- Auditoria de segurança / pentesting

03 Gestão e comunicação de incidentes

- Deteção - Classificação - Resposta – Recuperação
- Procedimentos - Coordenação com terceiros
- Notificação das autoridades
- Notificação dos afetados

04 Cadeia de fornecimento Serviços TIC

- REVISÃO DA RELAÇÃO CONTRATUAL
- Diligência devida: Avaliação de fornecedores

05 Compromisso de gestão

- Formação em matéria de segurança
- Decisões/Responsabilidade pela cibersegurança e riscos

Transposição (2025)

Auditoria interna - Medidas de controlo pelas autoridades

Melhoria contínua

Envolvimento dos quadros superiores

Artigo 20.1 Os órgãos de direção das entidades essenciais e importantes devem aprovar as medidas de gestão dos riscos de cibersegurança adotadas por essas entidades.

Artigo 20.2 Os membros dos órgãos de direção das entidades essenciais e importantes estão obrigados a seguir uma formação e incentivarão as entidades essenciais e importantes a oferecer periodicamente uma formação semelhante aos seus funcionários.

Artigo 32 ... Os Estados membros velarão para que as autoridades competentes estejam facultadas a solicitar que os órgãos jurisdicionais proíbam temporariamente qualquer pessoa que exerça responsabilidades de direção a nível de diretor-geral ou representante legal nessa entidade essencial de exercer funções de direção nessa entidade.

Os Estados membros garantirão que qualquer pessoa física responsável por uma entidade essencial ou que atue como representante da mesma, tome decisões em seu nome e exerça controlo sobre ela, e tenha competências para garantir o cumprimento da presente Diretiva. Os Estados membros velarão para que essas pessoas físicas possam ser consideradas responsáveis por incumprimento se não assegurarem o cumprimento da presente Diretiva.

Incumprimento grave de obrigações:

Responsabilidade pessoal dos cargos de direção

As autoridades competentes poderão impor uma proibição temporária para o exercício de cargos de direção, assim como a suspensão da autorização dos serviços ou atividades prestadas pela organização.

Regime sancionatório

Sanções administrativas

ESSENCIAIS: 10M € - 2% da atividade anual a nível mundial

IMPORTANTES: 7,5M € - 1,7% da atividade anual a nível mundial

Reclamações de danos

Eventuais pedidos das pessoas afetadas por incidentes de segurança

Não comunicação intencional de um incidente de segurança

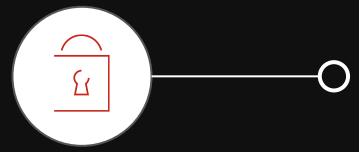
Os Estados-Membros podem impor sanções penais

Os nossos serviços

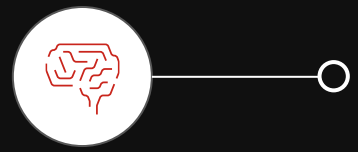
A nossa equipa

< 210	> 1200	36	18
sócios	profissionais	escritórios	países

Na Antas da Cunha ECIJA, ajudamos os nossos clientes na implementação da NIS2:



Criação / Adaptação do Sistema de Gestão da Segurança da Informação (SGSI) com base no risco, nas políticas e nos procedimentos do cliente, tanto do ponto de vista organizacional como técnico: controlo de acessos, encriptação, segurança dos recursos humanos, incidentes, continuidade da atividade, etc.



Formação e sensibilização do conselho de administração e dos órgãos de gestão para a segurança da informação.

Fornecedores e cadeia de abastecimento: Políticas de classificação de fornecedores, negociação de cláusulas específicas de cibersegurança com os fornecedores do cliente.

how can we help?

A ANTAS DA CUNHA ECIJA é a 1.ª Full AI Firm em Portugal. Uma Sociedade internacional, com 200+ profissionais, aposta na inovação e em equipas multidisciplinares. Integra a ECIJA, a maior rede ibero-americana e a aliança global Taylor Wessing, somando 3.000+ advogados em 30 países.

Ana Bastos
sócia
abastos@adceija.pt

Ana Catarina Silva
counsel
asilva@adceija.pt

Lídia Neves
counsel
lneves@adceija.pt

Márcia Dias Lomba
associada sénior
mlomba@adceija.pt

Diogo Moreira Ramos
associado sénior
dramos@adceija.pt

Diana Rocha Faria
associada sénior
dfaria@adceija.pt

Pedro Carrola Soares
associado
psoares@adceija.pt

Marta Albuquerque Coelho
associada
mcoelho@adceija.pt

YOUR FULL AI FIRM

www.adcecija.pt

FOLLOW US:

@antasdacunhaecija

@antasdacunhaecija