



## NIS 2 Overview

# PROGRAMA

## CONTEÚDOS

1

O contexto  
regulatório

2

O quadro legal e  
regulatório da  
Cibersegurança

3

A Diretiva NIS 2

4

Impactos

# 01 | O CONTEXTO REGULATÓRIO

# A Economia Digital e os catalisadores do risco

A digitalização da economia

Utilização de novas tecnologias e ferramentas – IoT, IA, 5G, *big data* e *online tracking*

Sofisticação dos incidentes e ciberataques

Maior dependência de terceiros (*supply chains*)

Ambientes de armazenamento e transferência de dados mais complexos

A necessidade de preservar informação sensível por longos períodos

Partilha de grandes volumes de dados

Transferência de dados para países terceiros

# A resposta legislativa

**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**



02

## O QUADRO LEGAL E REGULATÓRIO DA CIBERSEGURANÇA

# Regime Jurídico da Segurança do Ciberespaço



## Diretiva NIS 1

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



## Lei da Cibersegurança

**Lei n.º 46/2018**, de 13 de agosto, que estabeleceu o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148,



## Decreto-Lei da Cibersegurança

**Decreto-Lei n.º 65/2021**, de 30 de julho, que regulamenta a Lei da Cibersegurança



## Regulamento n.º 183/2022, de 21 de fevereiro

Regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança

# Regime Jurídico da Segurança do Ciberespaço



Obrigações de  
segurança das redes e  
dos sistemas de  
informação



Obrigações de  
notificação de  
incidentes de segurança  
com impacto relevante  
ou substancial



Notificação  
voluntária de incidentes

# 03

# A Diretiva NIS 2

# Reforço da legislação aplicável

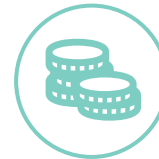


## Diretiva NIS 2

Alargamento do âmbito, 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

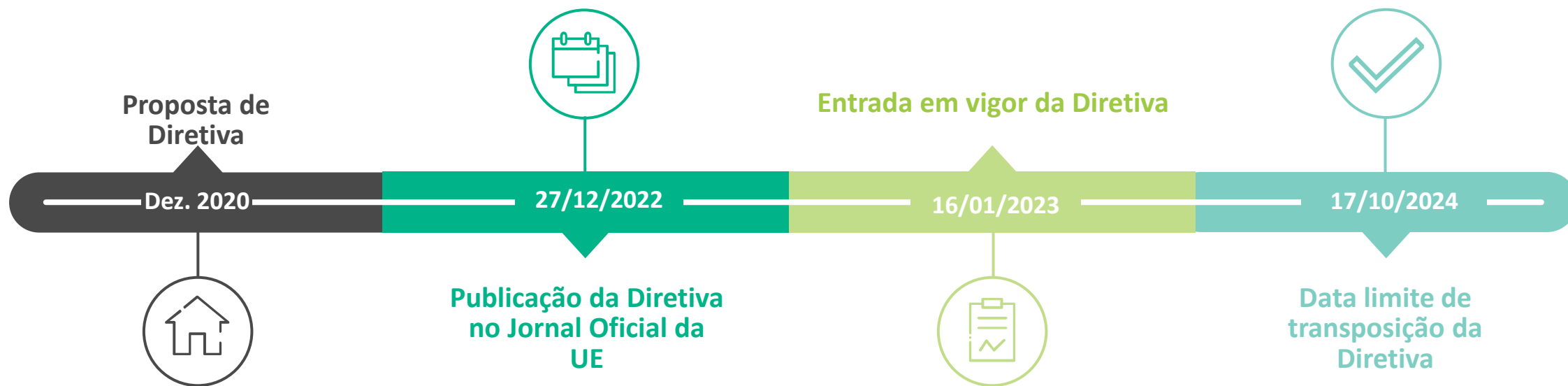
## Diretiva quanto à resiliência de infraestruturas críticas



## Regulamento DORA (*Digital Operational Resilience Act*)

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

# Diretiva NIS 2



Apesar de parecer uma realidade distante, as **alterações provocadas por esta Diretiva** são de tal forma profundas, que a preparação deve **iniciar-se o mais cedo possível**



# Diretiva NIS 2



Estratégia nacional  
de cibersegurança

Divulgação  
Coordenada da  
Vulnerabilidade



Grupo de  
Cooperação e Rede  
Europeia de  
Organizações de  
Ligação para crises  
cibernéticas (EU-  
CyCLONe)

Supervisão



Partilha de  
informação

# 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

# Diretiva NIS

Administração pública

Operadores de  
infraestruturas crítica

## Operadores de serviços essenciais

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

Pontos de troca de  
tráfego, prestadores de  
serviços de DNS e  
registos de nomes de  
domínio de topo

Eletricidade, petróleo e  
gás

Instalações de prestação  
de cuidados de saúde

Bancário e  
infraestruturas de  
mercado financeiro

Fornecimento e  
distribuição de água  
potável

## Prestadores de serviços digitais

- Mercados em linha
- Motores de pesquisa  
em linha
  - Serviços de  
computação em  
nuvem



# Diretiva NIS 2

## Operadores de serviços essenciais

### Infraestruturas do mercado financeiro

### Transporte

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

Bancário e infraestruturas de mercado financeiro

### 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**

### Espaço

**Tratamento de águas residuais**

+ Administração Pública

## Entidades importantes

**Serviços postais**

**Gestão de resíduos**

**Manufatura, produção e distribuição de químicos**

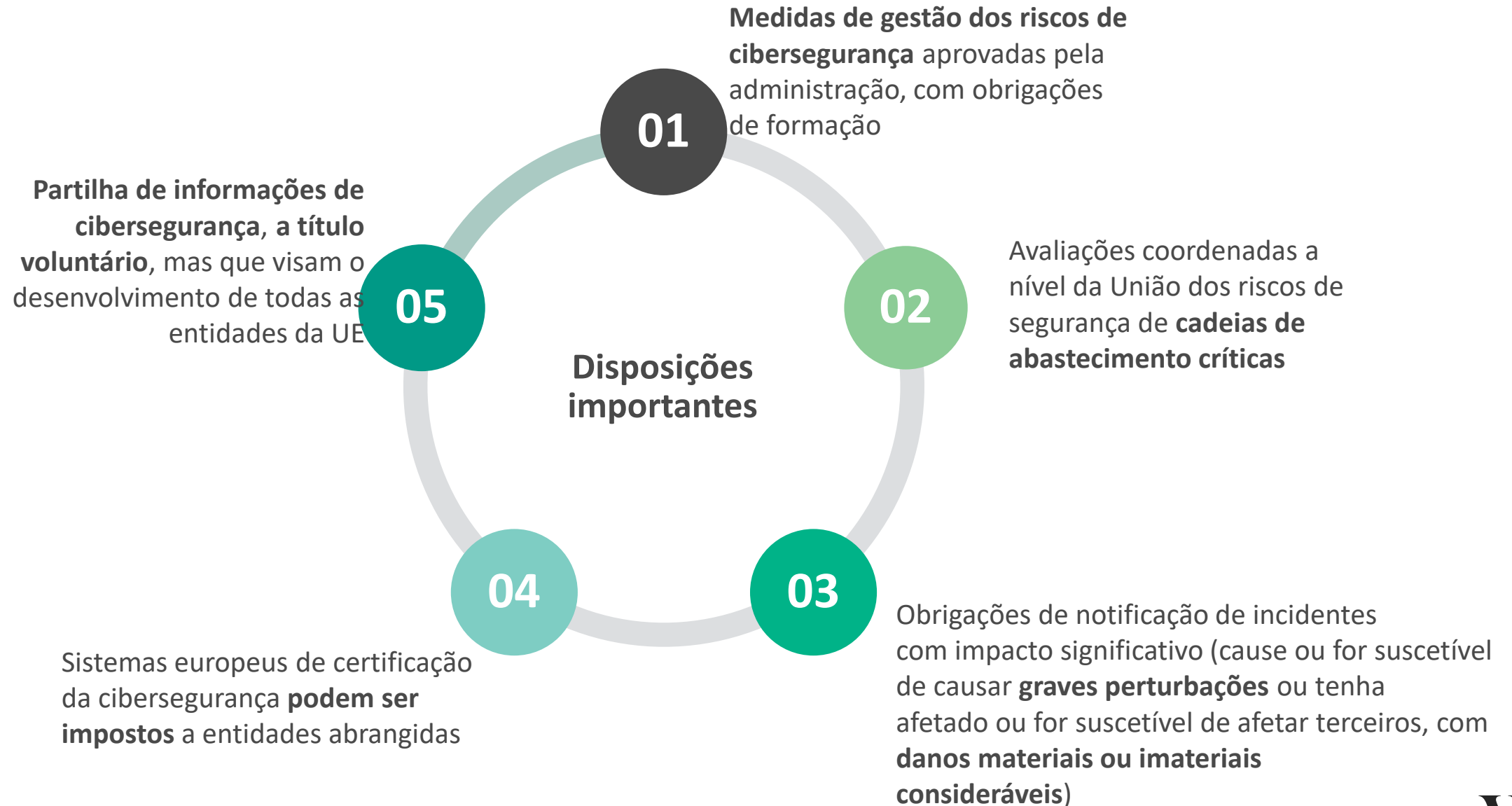
**Produção, processamento e distribuição de comida**

**Indústria transformadora**

**Operadores digitais de marketplaces, motores de pesquisa e plataformas sociais**

**Organismos de investigação**

# Diretiva NIS 2



# Gestão de riscos de cibersegurança

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 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

- **Aprovação e supervisão** da aplicação das medidas de gestão dos riscos de cibersegurança
- **Responsabilização** por infrações cometidas pela organização



- **Frequência regular em ações de formação**, de forma a conseguirem identificar os riscos de cibersegurança e avaliar as medidas de gestão destes riscos, bem como o seu impacto nos serviços prestados pela organização

# Notificação de incidentes



## Notificação de incidentes



### Alerta rápido

Emitido sem demora injustificada e, em qualquer caso, no prazo de 24 horas após a tomada de conhecimento do incidente, indicando se existem suspeitas de que o incidente significativo foi provocado por atos ilícitos ou maliciosos e se é suscetível de ter um impacto transfronteiriço.



### Notificação do incidente

Emitida sem demora injustificada e o mais tardar 72 horas depois de se ter tomado conhecimento do incidente significativo, com o objetivo, nomeadamente, de: (i) atualizar as informações transmitidas no âmbito do alerta rápido; e de (ii) fornecer uma avaliação inicial do incidente significativo



### Relatório intercalar

Emitido a pedido do CSIRT ou da autoridade nacional competente, destacando as atualizações importantes do estado da gestão do incidente e crises, destacando as atualizações importantes do estado da gestão do incidente e crises



### Relatório final

Emitido no prazo de um mês após o incidente significativo ter sido resolvido, devendo incluir uma descrição exaustiva do incidente

# 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



# Diretiva NIS 2



## 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

# 04 Impacto

# Para fazer face à complexa teia regulatória



**ANTECIPAÇÃO**

**CAPACITAÇÃO**



**IMPLEMENTAÇÃO**

- 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

Esta apresentação foi preparada para a Sessão “NIS 2: Cibersegurança na União Europeia” da APDC & VdA | Digital Union, no dia 2 de abril de 2024. A apresentação não deverá, total ou parcialmente, incluindo texto e/ou imagem, ser facultada a qualquer pessoa que não tenha estado presente na sessão, sem o nosso prévio consentimento por escrito. A apresentação não deverá também ser reproduzida ou disponibilizada em qualquer contexto, incluindo a sua disponibilização online, sem o nosso prévio consentimento por escrito.



**vda** VIEIRA DE ALMEIDA

[www.vda.pt](http://www.vda.pt)