

NIS2: Cibersegurança para além da tecnologia

Governança, risco e conformidade das organizações.



Um novo nível de exigência em cibersegurança

A Diretiva NIS2 reforça as obrigações das organizações em matéria de **cibersegurança, gestão do risco e governação**, tornando estas matérias uma responsabilidade que ultrapassa a dimensão estritamente tecnológica.

As entidades abrangidas passam a estar sujeitas a requisitos acrescidos requisitos em matéria de governação, gestão do risco de cibersegurança, notificação de incidentes e segurança da cadeia de abastecimento.

A sua organização está abrangida?

A NIS2 aplica-se, em regra, a **médias e grandes empresas que operam em setores essenciais ou importantes**, podendo, em determinados setores críticos, ser aplicável independentemente da dimensão da organização.

A aplicabilidade deve, contudo, ser analisada caso a caso, considerando fatores como o **setor, a dimensão e as atividades desenvolvidas em concreto**.

Mesmo organizações que não são tradicionalmente associadas a setores regulados podem ficar abrangidas quando as suas operações dependam significativamente de sistemas digitais.

Entre os setores potencialmente abrangidos encontram-se:

- Energia, transportes e saúde;
- Banca e infraestruturas do mercado financeiro;
- Água e águas residuais;
- Infraestruturas digitais e gestão de serviços TIC;
- Administração Pública e espaço;
- Serviços postais e de estafeta;
- Gestão de resíduos e produtos químicos;
- Produção alimentar e indústria transformadora;
- Prestadores de serviços digitais;
- Investigação.

O que passa a ser exigido?

As organizações abrangidas devem adotar medidas adequadas para responder às novas exigências, nomeadamente ao nível de:

- **Gestão do risco de cibersegurança;**
- **Governação e supervisão** pelos órgãos de administração;
- **Resposta e notificação de incidentes** dentro dos prazos aplicáveis;
- Segurança da cadeia de abastecimento;
- Políticas, procedimentos e mecanismos internos de controlo adequados.



O que implica a violação da NIS2

O incumprimento das obrigações pode determinar a aplicação de **coimas até €10.000.000 ou 2% do volume de negócios global anual**, bem como a **responsabilização pessoal dos membros dos órgãos de administração**, incluindo a possibilidade de proibição do exercício de funções de gestão.

Da avaliação à implementação

A preparação para a NIS2 deverá começar pela identificação do enquadramento da organização e evoluir para uma análise concreta do seu nível de conformidade:

1. Avaliar a aplicabilidade e classificação

Analisar o setor, dimensão e atividades desenvolvidas, determinar o enquadramento da entidade e apoiar o respetivo registo junto do Centro Nacional de Cibersegurança.

2. Avaliar o nível de conformidade

Rever a documentação existente, incluindo políticas, procedimentos, contratos, quadro de governação e procedimentos de resposta a incidentes.

3. Identificar gaps e prioridades

Mapear lacunas de conformidade e os riscos associados, definir as medidas de mitigação e um plano de ação com prioridades de atuação.

4. Apoiar a implementação

Preparar ou aperfeiçoar a documentação e as medidas de governação necessárias, em coordenação com especialistas em cibersegurança.

Assessoria em conformidade com a NIS2

A Andersen apoia as organizações ao longo do processo de conformidade com a NIS2, desde a avaliação da aplicabilidade e classificação da entidade até à identificação de gaps, definição de prioridades e implementação das medidas jurídicas e de governação necessárias.

A abordagem integrada permite articular as exigências jurídicas e regulatórias com as vertentes de cibersegurança e gestão do risco, apoiando as organizações na construção de um modelo de conformidade adequado à sua atividade e exposição.

Para mais informações, por favor, contacte:



Daniel Torres Gonçalves

Sócio | Corporate e M&A
daniel.goncalves@pt.andersen.com



Isabel Martínez Moriel

Sócia | Corporate e M&A
isabel.martinez@es.andersen.com



João Sousa Guimarães

Sócio | Corporate e M&A
joao.guimaraes@pt.andersen.com



Gonçalo Gil Barreiros

Sócio Local | Corporate e M&A
goncalo.barreiros@pt.andersen.com



Augusto Almeida Correia

Diretor | Corporate e M&A
augusto.correia@pt.andersen.com