

IMPLEMENTAÇÃO NACIONAL DAS EXIGÊNCIAS DA NIS 2

NOVO REGIME DE CIBERSEGURANÇA

João Vitorino, Pedro Ramalho de Almeida e Bernardo Pedro Santana

SUMÁRIO

O novo Regime Jurídico da Cibersegurança transpõe a Diretiva NIS 2 e alarga de forma significativa o universo de entidades sujeitas a obrigações reforçadas. Introduz deveres acrescidos para os órgãos de administração e impõe requisitos mínimos de gestão de risco, acompanhados de novas regras de identificação, reporte e controlo. Prevê ainda mecanismos de supervisão distintos para Entidades Essenciais e Entidades Importantes, bem como um quadro sancionatório mais exigente. O regime entra em vigor 120 dias após a publicação e a sua aplicação prática dependerá das instruções técnicas a emitir pelo CNCS e pelas autoridades setoriais.

NOVO ENQUADRAMENTO LEGAL

O novo Regime Jurídico da Cibersegurança (“**RJCS**”) aprovado pelo Governo, transponde a Diretiva NIS 2, reforça as obrigações das entidades públicas e privadas que desempenham funções essenciais ou importantes para o funcionamento da economia e da sociedade e alarga significativamente o número de entidades abrangidas.

Âmbito e Entidades Abrangidas

De facto, o RJCS abrange agora um número alargado de entidades, que inclui uma parte significativa da Administração Pública, nomeadamente os serviços técnicos e administrativos dos órgãos de soberania e entidades com elevado grau de integração digital. As entidades abrangidas agrupam-se em três categorias:

- (I) **Entidades Essenciais:** Entidades de setores críticos que excedem os limiares de médias empresas, empresas de comunicações eletrónicas classificadas como médias empresas e prestadores

qualificados de serviços de confiança, registos de TLD e prestadores de DNS. A qualificação também depende do grau de exposição a riscos e do impacto potencial.

- (2) Entidades Importantes: Entidades dos mesmos setores críticos que não preenchem os critérios das Entidades Essenciais; e
- (3) Entidades Públicas Relevantes: Categoria que abrange entidades públicas que não se enquadram nos dois grupos anteriores, distribuídas pelos Grupos A e B consoante a respetiva dimensão.

O RJCS exclui entidades públicas que atuam nos domínios da segurança nacional, da segurança pública, da defesa e dos serviços de informações, incluindo entidades com funções de investigação criminal e órgãos de polícia criminal.

Novas obrigações para as empresas

As entidades abrangidas devem identificar-se na plataforma eletrónica do Centro Nacional de Cibersegurança (“**CNCS**”) no prazo de 30 dias após o início da atividade ou, se já se encontrarem em funcionamento, no prazo de 60 dias após a disponibilização dessa plataforma, devendo manter a informação sempre atualizada.

A nova lei atribui aos órgãos de administração responsabilidade direta na gestão dos riscos de cibersegurança, e a falta de supervisão adequada pode gerar responsabilidade e sanções para os administradores.

Os órgãos de gestão das EE e das EI assumem obrigações reforçadas de aprovação e controlo das medidas de cibersegurança, incluindo a formação regular.

Obrigações de gestão de risco

As entidades essenciais e importantes devem adotar medidas técnicas e organizativas proporcionais ao nível de risco da sua atividade e implementar um sistema de gestão de riscos que abranja todos os ativos e sistemas necessários à continuidade dos serviços. As medidas devem seguir as orientações e matrizes de risco do CNCS e refletir os progressos técnicos aplicáveis.

O RJCS estabelece requisitos mínimos de segurança, incluindo políticas de gestão de risco, continuidade de operações, controlo de acessos e utilização de autenticação multifator. Exige ainda a avaliação e documentação do risco residual e a adoção célere das medidas corretivas necessárias. Cada entidade deve elaborar um relatório anual, designar um responsável pela cibersegurança e manter um ponto de contacto permanente com disponibilidade contínua.

Cria também um sistema nacional de certificação de cibersegurança para tecnologias da informação e comunicação, que pode ser utilizado para demonstrar a adequação das medidas implementadas e facilitar os processos de conformidade.

Notificação de incidentes

O novo regime fixa prazos mais curtos para a comunicação de incidentes significativos e violações de segurança. As entidades abrangidas devem notificar incidentes significativos à autoridade competente através de três etapas: notificação inicial em 24 horas, atualização em 72 horas e relatório final até 30 dias úteis após o fim do impacto.

Papel do Centro Nacional de Cibersegurança

O CNCS exerce a coordenação nacional da segurança do ciberespaço e assume novas competências de supervisão, auditoria, fiscalização e emissão de orientações técnicas. A intensidade da supervisão varia conforme a classificação da entidade como essencial ou importante. As autoridades setoriais colaboram com o CNCS e exercem poderes de controlo nos respetivos setores.

As EE ficam sujeitas a supervisão contínua, incluindo auditorias, inspeções e testes. As EI ficam, em regra, sujeitas a supervisão reativa, sendo fiscalizadas sobretudo após incidentes ou indícios de incumprimento.

O RJCS estabelece coimas mais elevadas para infrações graves ou muito graves, prevendo limites até €10 M ou 2% do volume de negócios para EE e até €7 M ou 1,4% do volume de negócios para EI, alinhando Portugal com o modelo sancionatório da Diretiva NIS 2.

Entrada em vigor e período de transição

O novo RJCS produz efeitos 120 dias após a publicação. O CNCS e as autoridades setoriais preparam agora instruções técnicas e normas complementares que concretizam os vários aspetos operacionais do regime.

© 2025 MACEDO VITORINO

SOBRE A MACEDO VITORINO

A MACEDO VITORINO é uma prestigiada sociedade de advogados. Assessoramos clientes portugueses e estrangeiros num amplo leque de setores de atividade, incluindo banca, distribuição,

indústria, energia, tecnologia, media e telecomunicações e projetos. Temos ainda estado envolvidos em processos e na reestruturação de empresas.

Somos conhecidos pela nossa abordagem profissional e empresarial aos assuntos mais complexos e difíceis.

A MACEDO VITORINO mantém relações de correspondência e de parceria com algumas das mais prestigiadas sociedades de advogados internacionais da Europa, Estados Unidos, Brasil e Ásia, o que nos permite prestar aconselhamento em operações internacionais de forma eficiente.

Se pretende saber mais sobre a MACEDO VITORINO por favor visite o nosso site www.macedovitorino.com.

INFORMAÇÃO IMPORTANTE

As opiniões expressas neste artigo são de natureza geral e não devem ser consideradas como aconselhamento profissional. Caso necessite de aconselhamento jurídico sobre estas matérias, deve contactar um advogado. Se for cliente da MACEDO VITORINO, pode contactar-nos por email para mv@macedovitorino.com.