VIEIRA DE ALMEIDA

COMUNICAÇÕES, PROTEÇÃO DE DADOS E TECNOLOGIA

REGULAMENTAÇÃO DO REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

VdA EXPERTISE

Agosto 2021

Foi publicada a regulamentação do Regime Jurídico da Segurança do Ciberespaço com impacto nos operadores de infraestruturas críticas e de serviços essenciais, nos prestadores de serviços digitais e na Administração Pública

Entrou em vigor no dia 9 de agosto de 2021 o tão aguardado Decreto-Lei n.º 65/2021 que veio **regulamentar** o **Regime Jurídico da Segurança do Ciberespaço** (Lei n.º 46/2018) e **definir** as **obrigações em matéria de certificação da cibersegurança**, em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

Este diploma vem responder a inúmeras questões que estavam por endereçar no contexto da Lei n.º 46/2018, estabelecendo **obrigações exigentes** para as entidades abrangidas relativamente aos:

- **requisitos de segurança das redes e sistemas de informação**; e
- **requisitos de notificação de incidentes** que afetem a segurança das redes e dos sistemas de informação.

Devem cumprir os requisitos estabelecidos os **operadores de infraestruturas críticas** (entidades públicas ou privadas que operam uma infraestrutura crítica), os **operadores de serviços essenciais** (nos setores da energia, transportes, bancário e financeiro, saúde, água e infraestruturas digitais), os **prestadores de serviços digitais** (comércio online, motores de pesquisa online e computação em nuvem) e as entidades da **Administração Pública**. Em particular, os requisitos de segurança aplicáveis aos prestadores de serviços digitais são definidos por regulamento de execução da Comissão Europeia.

O não cumprimento das obrigações estabelecidas, pode gerar:

- contraordenações **muito graves** → coimas que variam, para as pessoas coletivas, entre **€25.000** e **€50.000** (no caso de incumprimento das obrigações relativas aos requisitos de segurança)

contraordenações **graves** → coimas que variam, para as pessoas coletivas, entre **€9.000** e **€3.000** (no caso de incumprimento das obrigações de notificação)

O diploma vem ainda permitir a implementação de um **quadro nacional de certificação da cibersegurança** pelo **CNCS** (Centro Nacional de Cibersegurança), que atuará como a Autoridade Nacional de Certificação da Cibersegurança. O CNCS deverá estabelecer as disposições necessárias à elaboração e execução de esquemas específicos de certificação da cibersegurança relativos a produtos, serviços e processos de tecnologias de informação e comunicação.

Os requisitos previstos no Decreto-Lei n.º 65/2021 constituem um mínimo a assegurar pelas entidades abrangidas, não prejudicando as regras que, em função da natureza das entidades e dos setores em que atuem, possam vir a ser estabelecidas por outras autoridades, nem tão-pouco disposições que resultem de outros diplomas (como é o caso, desde logo, das obrigações aplicáveis aos prestadores de serviços digitais). Também o CNCS pode emitir instruções técnicas complementares em matéria de requisitos de segurança e de notificação de incidentes.

A **densificação das obrigações de cibersegurança**, que se apresenta **na página seguinte deste Flash**, procura assegurar um nível elevado de segurança das redes e dos sistemas de informação que sustentam o uso de tecnologias cada vez mais disruptivas (como a Inteligência Artificial ou a Internet das Coisas), para que decorra num ambiente de confiança. É inegável que o cumprimento das obrigações de cibersegurança permitirá não só o compliance legal pelas organizações, como também lhes proporcionará significativos benefícios a nível reputacional e comportamental.

Impõe-se, assim, que as organizações comecem a preparar o quanto antes os seus sistemas e equipas para a implementação deste novo regime, tornando-se mais resilientes face às ameaças internas e externas que afetam o ciberespaço e evitando a aplicação de coimas severas.

Principais obrigações

De forma sucinta, prevê-se que as entidades abrangidas

Ponto de contacto permanente **	Indiquem um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS.
Responsável de segurança **	Designem um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.
Inventário dos ativos *	Elaborem e mantenham atualizado um inventário de todos os **ativos essenciais** para a prestação dos seus serviços, com informação definida em instruções técnicas emitidas pelo CNCS, que deve ser assinado pelo responsável de segurança e comunicado ao CNCS.
Plano de segurança **	Elaborem e mantenham atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança.
Relatório Anual *	Elaborem um relatório anual, com informação sobre as atividades desenvolvidas em matéria de segurança e os incidentes de segurança ocorridos, que deve ser remetido ao CNCS em janeiro de cada ano e assinado pelo responsável de segurança.
Medidas de segurança ***	Adotem medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação por si utilizados, em linha com a análise dos riscos realizada e tendo em conta os progressos técnicos mais recentes, utilizando normas e especificações técnicas internacionalmente aceites.
Análise dos riscos ***	Realizem e documentem uma análise dos riscos relativa a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação e/ou que garantam a prestação de serviços (dependendo das entidades em causa). Esta análise poderá ser de **âmbito global** ou de **âmbito parcial**, de acordo com os requisitos e a periodicidade previstos na lei.
Notificação de incidentes **	Notifiquem o CNCS da ocorrência de incidentes com um impacto relevante ou substancial. Por cada incidente que deva ser objeto de notificação, a entidade deve submeter: (i) uma **notificação inicial**, (ii) uma **notificação de fim de impacto** relevante ou substancial, e (iii) uma **notificação final**, com prazos específicos previstos no diploma. Estas notificações deverão ser articuladas com as notificações de violação de dados pessoais ao abrigo do RGPD, bem como com outras notificações a reguladores sectoriais.

* Obrigação atualmente aplicável
** Obrigação aplicável a partir de novembro de 2021
*** Obrigação aplicável a partir de agosto de 2022

Contactos

MAGDA COCCO
MPC@VDA.PT

INÊS ANTAS DE BARROS
IAB@VDA.PT

HELENA CORREIA MENDONÇA
HCM@VDA.PT

MARIA DE LURDES GONÇALVES
MLG@VDA.PT