NIS 2: "UMA EVOLUÇÃO (E NÃO UMA REVOLUÇÃO)" DA SEGURANÇA DAS REDES E SISTEMAS DE INFORMAÇÃO

POR MARIA BEATRIZ FERNANDES

A ATUALIZAÇÃO DA NETWORK AND INFORMATION SECURITY (NIS), O "PRIMEIRO DIPLOMA LEGISLATIVO DA UNIÃO EUROPEIA A ABORDAR O TEMA DA CIBERSEGURANÇA", AUMENTA O SEU ÂMBITO E ABRANGÊNCIA, REFORÇA PRINCÍPIOS CONSIDERADOS ESSENCIAIS À CIBER-RESILIÊNCIA, E CRIA GRUPO DE APOIO À COORDENAÇÃO ESTRATÉGICA DE INICIATIVAS DE CIBERSEGURANÇA ENTRE ESTADOS-MEMBROS

O fim de um ano e o início de um novo levantou ondas na legislação europeia no âmbito da cibersegurança e resiliência das redes e sistemas de informação. Oficializada com a publicação no Jornal Oficial da União Europeia, a diretiva 2022/2555 – ou NIS 2 – entrou em vigor ao vigésimo dia da publicação, a 16 de janeiro, dia a partir do qual os Estados-membros dispõem no máximo de 21 meses para proceder à transposição para o direito nacional. O processo culmina no dia 17 de outubro de 2024, no qual deverão ser adotadas e publicadas as medidas necessárias para cumprir a diretiva.

É de notar, contudo, que o Conselho Europeu lançou uma recomendação em dezembro, pedindo que a transposição das novas regras fosse acelerada e a aplicação das novas medidas começasse antes do limite temporal findar, dada a urgência dos temas.

DE ONDE VEM

Sucederam-se inúmeras discussões para a reformulação da NIS, o "primeiro diploma legislativo da União Europeia a abordar o tema da cibersegurança", de acordo com Daniel Reis, Sócio da DLA Piper. No caso português, a NIS resultou na Lei 46/2018, de 13 de agosto, que floresceu no Regime Jurídico da Segurança do Ciberespaço, resumidamente, "um diploma fundador de um regime jurídico especialmente dedicado à cibersegurança em Portugal", declarou Ricardo Henriques, sócio da Abreu Advogados.

Mas a revolução regulamentar que despoletou da NIS não ficou por aqui. É da responsabilidade da diretiva a criação da Estratégia Nacional de Segurança no Ciberespaço, assim como do Conselho Superior de Segurança do Ciberespaço, que, entre outras competências, controla a sua implementação, e a definição do Centro Nacional de Cibersegurança enquanto Autoridade Nacional de Cibersegurança.

Para além de "definir toda a orgânica nacional no que respeita a este tema", comenta


RICARDO HENRIQUES, SÓCIO DA ABREU ADVOGADOS

Ricardo Henriques, estabeleceu as necessidades de notificação no caso de incidentes, requisitos de segurança, e uma série de contraordenações e sanções pelos possíveis incumprimentos, "reforçando a seriedade do tema da cibersegurança no panorama nacional". Continua: "será seguro dizer que a NIS foi de vital importância para a construção de um panorama jurídico de cibersegurança em Portugal", e que "promoveu e auxiliou a implementação de uma cultura de ciber-higiene nas organizações", acrescenta Alexandra Palma, Information Security Consultant da Integrity.

Todavia, do ponto de vista prático, "apresentou algumas lacunas", menciona a consultora, que a nova diretiva veio suprir. "Este aspeto é sustentado de forma explícita no seu considerando 2, assumindo a identificação de "deficiências intrínsecas que a impedem de responder de forma eficaz a desafios atuais e emergentes no domínio da cibersegurança, uma vez que se revelou demasiado ampla", elucida.

PARA ONDE VAI

O novo diploma revoga e substitui a diretiva sobre segurança das redes e da informação SRI, Diretiva 2016/1148, e propõe-se a:

• **Fazer melhorias na gestão dos riscos de cibersegurança, através, por exemplo, da introdução de novas obrigações de *reporting*.**

Segundo o artigo 21, sobre medidas de gestão dos riscos de cibersegurança, entidades essenciais e importantes devem tomar medidas técnicas, operacionais e organizativas adequadas e proporcionais para gerir os riscos colocados à segurança das redes e dos sistemas de informação. Tudo isto, sob uma abordagem holística, de todos os riscos, que vise proteger as redes e os sistemas de informação e o ambiente físico desses sistemas contra incidentes.

> NO CASO PORTUGUÊS, A NIS RESULTOU NA LEI 46/2018, DE 13 DE AGOSTO, QUE FLORESCEU NO REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO, RESUMIDAMENTE, "UM DIPLOMA FUNDADOR DE UM REGIME JURÍDICO ESPECIALMENTE DEDICADO À CIBERSEGURANÇA EM PORTUGAL"
>
> RICARDO HENRIQUES, SÓCIO DA ABREU ADVOGADOS

• Estabelecer obrigações adicionais de supervisão para as autoridades competentes dos Estados-membros, e de notificação de incidentes, com uma maior urgência (prazo definido de 24 horas para o aviso de um incidente significativo e 72 horas para a comunicação de incidentes).

É de ressalvar o artigo 20, sobre *governance*, que indica que os órgãos de gestão de entidades essenciais e importantes devem aprovar as medidas de gestão do risco de cibersegurança tomadas por essas entidades, supervisionar a sua implementação e "podem ser responsabilizadas por infrações".

O artigo reitera, ainda, o princípio da formação e literacia como meio de resiliência. Assim, os Estados-membros deverão assegurar que os "membros dos órgãos de gestão de entidades essenciais e importantes sejam obrigados a seguir a formação", e incentivá-los a oferecerem formação aos trabalhadores regularmente.

• Aumentar a abrangência de setores e de tipos de entidades.

Anteriormente direcionado a operadores de serviços essenciais e críticos, e alguns operadores de

serviços digitais, o diploma passa, agora, a incluir a "energia, espaço transportes, financeiro, saúde, água, telecomunicações, serviços cloud, nomes de domínio, data centers, administração pública, postal, resíduos, químicos, alimentar, eletrónica e automóvel, redes sociais, motores de busca e comércio eletrónico", diz Daniel Reis;

Com o aumento da abrangência, inúmeras empresas terão de adaptar os seus procedimentos às novas regras. De acordo com Daniel Reis, este reflete o maior impacto. Atualmente, ainda não existe qualquer versão ou minuta da lei portuguesa que transponha a nova regulamentação.

Adicionalmente, aquando da transposição, cada Estado-membro pode alargar o seu âmbito de aplicabilidade.

• Criar Equipas de Resposta a Incidentes de Segurança Informática (CSIRT), que "garantam disponibilidade de serviços de comunicações", responsáveis por monitorizar ciberameaças, vulnerabilidades e incidentes a nível nacional, intervir em caso de acidentes e proceder a análises dinâmicas dos riscos e dos incidentes, bem como desenvolver o conhecimento situacional em cibersegurança";

• Reforçar as atribuições da ENISA (o regulador europeu);

• Instituir que se uma entidade não estiver estabelecida na Europa, mas fornecer serviços no seio do território, deverá designar um representante num dos Estados-membros da UE, submetendo-se à legislação do país em causa. Na ausência de um representante, qualquer Estado-membro no qual a entidade presta serviços pode tomar medidas legais por infração à presente diretiva;

• Criar um grupo de cooperação para facilitar a coordenação estratégica no âmbito da diretiva, com a EU-CyCLONe.

A diretiva veio estabelecer a European Cyber Crises Liaison Organisation Network para apoiar uma gestão coordenada de incidentes e crises de cibersegurança de grande escala europeia a nível operacional e "assegurar o intercâmbio regular de informações entre os Estados-membros", explica Ricardo Henriques. Porque as ameaças e incidentes de segurança "não conhecem fronteiras", o que se pretende com a nova rede é "melhorar a integração e cooperação entre os diferentes reguladores europeus", continua Daniel Reis (DLA Piper).


DANIEL REIS, SÓCIO DA DLA PIPER

"Estas competências evidenciam o sentido de urgência e missão da União Europeia em continuamente abrir espaço para um mercado único seguro e eficaz, sem risco para consumidores e internautas em geral, alinhando-se em concreto com a estratégia de já alguns anos", acredita Ricardo Henriques.

> PORQUE AS AMEAÇAS E INCIDENTES DE SEGURANÇA "NÃO CONHECEM FRONTEIRAS", O QUE SE PRETENDE COM A NOVA REDE É "MELHORAR A INTEGRAÇÃO E COOPERAÇÃO ENTRE OS DIFERENTES REGULADORES EUROPEUS",
>
> DANIEL REIS, SÓCIO DA DLA PIPER

> A NIS 2 "TROUXE ALTERAÇÕES POUCO SUBSTANCIAIS. HOUVE UMA EVOLUÇÃO (E NÃO UMA REVOLUÇÃO), E APESAR DE ESTARMOS PERANTE UMA REVOGAÇÃO EXPRESSA DA NIS, O ESPÍRITO DA MESMA PERMANECE, A SUA ESPINHA DORSAL MANTÉM-SE"
>
> ALEXANDRA PALMA, INFORMATION SECURITY CONSULTANT DA INTEGRITY

ALEXANDRA PALMA, INFORMATION SECURITY CONSULTANT DA INTEGRITY

O QUE SE SEGUE?

A Information Security Consultant da Integrity acredita que, "ainda que tenha ocorrido um claro alargamento de âmbito de aplicabilidade", a NIS 2 "trouxe alterações pouco substanciais. Houve uma evolução (e não uma revolução), e apesar de estarmos perante uma revogação expressa da NIS, o espírito da mesma permanece, a sua espinha dorsal mantém-se".

Face à atual evolução legislativa, "é prudente atuar antecipadamente", tendo em conta que as entidades que não estão abrangidas, podem, futuramente, vir a "constar do seu âmbito de aplicabilidade" ou até mesmo através do alargamento de âmbito no momento da transposição da diretiva para o ordenamento jurídico nacional, conta Alexandra Palma.

Presente num painel do Building the Future 2023, António Gameiro Marques, Diretor-Geral do Gabinete Nacional de Segurança, disse que a transposição da diretiva para a legislação nacional está em andamento. "Temos um plano", apresentado no dia 26 de janeiro a Mário de Campolargo, Secretário de Estado da Digitalização e Modernização Administrativa, "e o nosso objetivo é ter o estudo de impacto da NIS 2 no atual contexto legislativo e nas empresas até outubro deste ano", explicou. Depois, a lei deverá "fazer o seu caminho dentro do Governo e da Assembleia da República", visto que, "havendo necessidade de alterações na lei, há um processo legislativo mais complexo", conclui o responsável do GNS.

"Somos todos peças de um puzzle" e "temos o dever de cuidar de forma diligente e preventiva, para que em caso de incidente significativo os danos sejam minimizados e mitigados ao máximo, com as menores repercussões possíveis", remata a consultora. ◀