A DIRETIVA NIS2: O NOVO PANORAMA DA CIBER-RESILIÊNCIA

"Com a aproximação de um novo e exigente quadro legal, um puzzle complexo do qual a NIS 2 é só uma peça, as organizações devem começar um exercício (significativo) de preparação para esta nova realidade"

Inês Antas de Barros
Sócia da Vieira de Almeida

Na Era digital, a cibersegurança merece uma atenção sem precedentes, sendo as falhas de cibersegurança identificadas, pelo World International Forum, como um dos dez riscos mais prováveis e impactantes para a próxima década.

Não é, pois, de estranhar que, a nível europeu, a cibersegurança tenha conhecido desenvolvimentos consideráveis, com a aprovação, em 2020, da Estratégia da UE para a Cibersegurança, que inclui diferentes iniciativas, como a nova diretiva relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança em toda a União (Diretiva (UE) 2022/2555 – "NIS 2").

A NIS 2, em vigor desde 16 de janeiro de 2023 e a transpor para o ordenamento jurídico nacional até 17 de outubro de 2024, abrange vários sectores e reforça obrigações em sede de segurança da informação, procurando dar resposta coerente e complementar aos riscos atuais e futuros, desde os ciberataques até à criminalidade e às catástrofes naturais.

A NIS 2 alarga o âmbito de aplicação face à Diretiva NIS original, abrangendo todas as entidades que, na UE prestem serviços ou realizem atividades qualificadas como como "essenciais" ou "importantes" – incluindo no sector bancário, infraestruturas do mercado financeiro, fornecedores e infraestruturas digitais, gestão de serviços TIC, saúde, serviços postais, energia, transportes, espaço, indústria transformadora, certos tipos de produção e distribuição e Administração Pública.

A NIS 2 foca-se na gestão de risco, governance e responsabilização da Administração, devendo as entidades adotar exigentes metodologias de gestão de riscos de cibersegurança, que passam pela elaboração de políticas de análise e gestão de riscos, tratamento e notificação de incidentes, continuidade de atividades, procedimentos de avaliação da eficácia das medidas e formação. É também exigido que as entidades contemplem os riscos e obrigações em matéria de cibersegurança nas suas relações com os fornecedores.

Com o reforço dos poderes de supervisão e do quadro sancionatório (com coimas a ascender aos 10 000 000 EUR ou a 2% do volume de negócios a nível mundial, consoante o valor mais elevado), antecipar é a palavra de ordem.

Os temas de compliance e de natureza jurídica, crescentemente materiais neste domínio, são reforçados neste quadro legal. Nos incidentes de cibersegurança, as contingências associadas às coimas por incumprimento das obrigações de segurança e aos pedidos de indemnização de titulares afetados têm sido identificadas como críticas e ganharão ainda mais expressão com a NIS 2.

A experiência recente demonstra que um incidente de segurança acarreta avultados danos financeiros, operacionais, reputacionais e legais (responsabilidade contraordenacional, penal, civil, contratual e extracontratual das organizações), pontos centrais à abordagem que as organizações façam à cibersegurança - não só na resposta e gestão de um incidente, mas também no desenho e implementação de planos de ciber-resiliência.

Com a aproximação de um novo e exigente quadro legal, um puzzle complexo do qual a NIS 2 é só uma peça, as organizações devem começar um exercício (significativo) de preparação para esta nova realidade.

Para tal, importa desenvolver ou adaptar as estratégias de gestão de riscos cibernéticos, englobando todo o ecossistema da cibersegurança, de forma a identificar, gerir e reduzir os riscos jurídicos, técnicos, operacionais e de negócio – sendo essencial o *buy-in* da respetiva Administração, que passa a ter responsabilidades acrescidas nesta matéria. ■