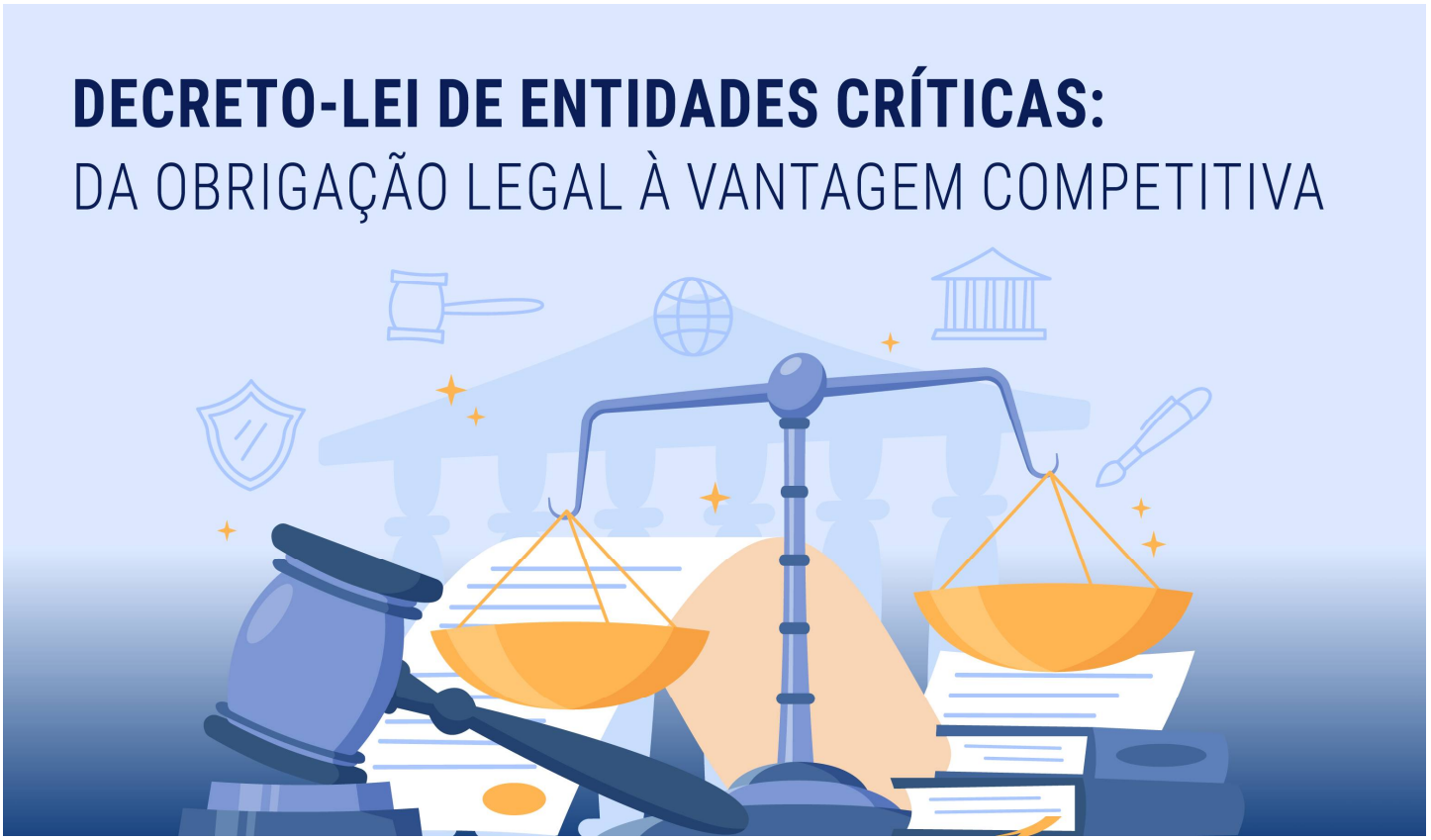
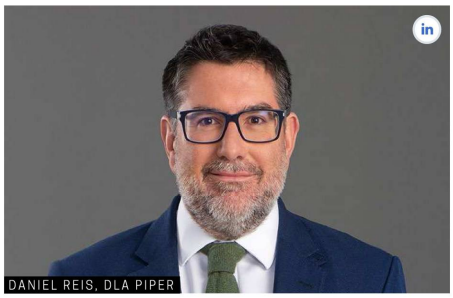

DECRETO-LEI DE ENTIDADES CRÍTICAS:
DA OBRIGAÇÃO LEGAL À VANTAGEM COMPETITIVA

POR INÊS GARCIA MARTINS

POR ENTRE A VAGA DE REGULAÇÃO QUE A EUROPA TEM ASSISTIDO, O NOVO DECRETO-LEI DE ENTIDADES CRÍTICAS (DECRETO-LEI N.º 22/2025) SURGE COMO PARADOXO PARA AS EMPRESAS PORTUGUESAS. MAIS DO QUE UM DESAFIO DE CONFORMIDADE, IMPÕE OBRIGAÇÕES QUE VÃO ALÉM DA CIBERSEGURANÇA E EXIGEM MUDANÇAS PROFUNDAS NA GESTÃO DO RISCO. A RESPOSTA NÃO É SIMPLES, SOBRETUDO QUANDO OS ESPECIALISTAS ALERTAM PARA UM NÍVEL MÍNIMO DE PREPARAÇÃO. MESMO ASSIM, ESTE NOVO ENQUADRAMENTO PODE TRANSFORMAR-SE DE OBRIGAÇÃO EM VANTAGEM COMPETITIVA PARA QUEM SOUBER ANTECIPAR-SE

Num cenário global de "policrise", marcado por ameaças híbridas, disrupções nas cadeias de abastecimento e a crescente sofisticação dos ciberataques, o panorama regulatório português prepara-se para uma mudança estrutural. A iminente implementação do Decreto-Lei n.º 22/2025, que estabelece o regime de resiliência das entidades críticas, é a resposta nacional a este desafio. Longe de ser apenas mais um diploma a arquivar, esta legislação, que transpõe a Diretiva (UE) 2022/2557 (Diretiva CER), representa uma redefinição fundamental da forma como as organizações vitais para o país devem encarar e gerir o risco. Para os profissionais de cibersegurança e gestão de risco, o desafio é claro: transformar uma complexa teia de obrigações numa alavanca estratégica para a resiliência operacional e o ganho competitivo.

O novo quadro legal, como resume de forma sucinta Daniel Reis, Sócio da DLA Piper, "cria um novo quadro jurídico para identificar, designar e reforçar a resiliência das entidades críticas nacionais e europeias, para garantir a continuidade de serviços essenciais. De forma simplista, vem criar obrigações para as entidades críticas". Esta aparente simplicidade esconde, no entanto, uma profundidade de mudança que vai muito além da cibersegurança, o que, por sua vez, exige uma abordagem integrada que poucas empresas em Portugal já praticam de forma sistemática.


DANIEL REIS, DLA PIPER

UMA VISÃO HOLÍSTICA DO RISCO

A principal novidade prática deste Decreto-Lei é a sua abrangência. Ao contrário de regimes como a NIS2, que se foca especificamente na segurança digital, esta legislação impõe uma gestão de risco que transcende as barreiras do digital e do físico, o que força uma colaboração sem precedentes entre diferentes departamentos.

O NOVO QUADRO LEGAL, "CRIA UM NOVO QUADRO JURÍDICO PARA IDENTIFICAR, DESIGNAR E REFORÇAR A RESILIÊNCIA DAS ENTIDADES CRÍTICAS NACIONAIS E EUROPEIAS, PARA GARANTIR A CONTINUIDADE DE SERVIÇOS ESSENCIAIS. DE FORMA SIMPLISTA, VEM CRIAR OBRIGAÇÕES PARA AS ENTIDADES CRÍTICAS".

Catarina Mascarenhas, Consultora da Abreu Advogados, detalha esta mudança de paradigma, e explica que as empresas vão enfrentar "um conjunto de obrigações que recaem sobre a entidade crítica, como um todo, enquanto organização, recursos humanos e modo de funcionamento, assente numa lógica de gestão de risco". Lógica essa que exige, segundo a especialista, uma "visão holística, integrada e coordenada perante um conjunto de ameaças e riscos que vão desde atos intencionais a catástrofes naturais e a emergências de saúde pública".

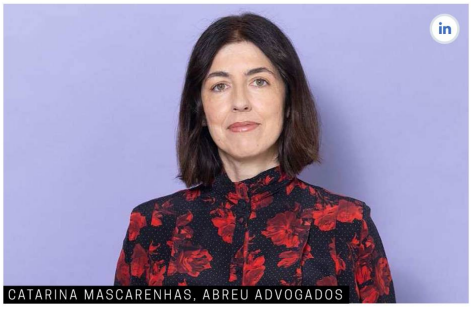
Isto significa que o CISO e o responsável pela segurança física, que em muitas organizações operam em silos, terão de se sentar à mesma mesa e desenvolver estratégias conjuntas. O plano de resiliência de um operador de infraestruturas de transportes, por exemplo, terá de contemplar tanto a defesa contra um ataque de ransomware que paralise os seus sistemas de logística, como a resposta a uma greve que afete a operação ou a um

evento climático extremo que danifique as suas infraestruturas.

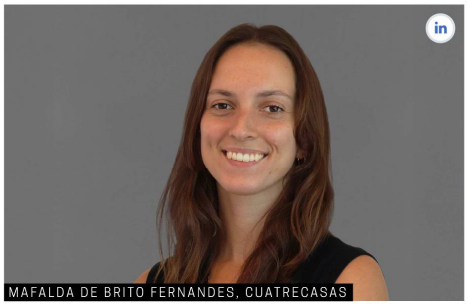
As obrigações são claras e exigentes: realizar avaliações de risco que abranjam todo o espectro de ameaças, elaborar planos de resiliência que contemplem medidas preventivas, de proteção, resposta e recuperação, e testá-los através de exercícios periódicos. Adicionalmente, a notificação de incidentes com impacto significativo deve ser feita no prazo máximo de 24 horas. Por fim, como nota Catarina Mascarenhas, estas entidades estão também "sujeitas a ações de fiscalização como auditorias e inspeções", o que eleva o nível de escrutínio e responsabilidade a um novo patamar.

O ROTEIRO PARA A DESIGNAÇÃO E O PUZZLE REGULATÓRIO

Uma das questões centrais para as empresas é saber se são abrangidas. O processo, conduzido pelo Conselho Nacional de Planeamento Civil de Emergência (CNPCE) em articulação com as entidades setoriais, tem um prazo definido. "A identificação e designação devem ocorrer até 17 de julho de 2026", clarifica José Maria Alves Pereira, Advogado Principal da Abreu Advogados. Os critérios para ser considerada "crítica" são cumulativos e incluem a prestação de serviços essenciais, a operação em território nacional e, crucialmente, a avaliação de que um incidente provocaria um "efeito perturbador significativo".


CATARINA MASCARENHAS, ABREU ADVOGADOS

"A NIS 2 É ESPECÍFICA PARA A CIBERSEGURANÇA, ENQUANTO O DECRETO-LEI N.º 22/2025 ADOTA UMA ABORDAGEM MAIS ABRANGENTE, INCLUINDO TANTO AMEAÇAS FÍSICAS COMO CIBERNÉTICAS"


MAFALDA DE BRITO FERNANDES, CUATRECASAS

Mafalda de Brito Fernandes, Advogada da Cuatrecasas, detalha que este impacto será avaliado com base em métricas concretas como "o número de utilizadores afetados, interdependências setoriais, impacto socioeconómico, quota de mercado e vulnerabilidades geográficas".

Para os profissionais de cibersegurança, a articulação deste regime com a Diretiva NIS2 é vital – não são regimes conflituantes, mas sim complementares. "A NIS 2 é específica para a cibersegurança, enquanto o Decreto-lei n.º 22/2025 adota uma abordagem mais abrangente, incluindo tanto ameaças físicas como cibernéticas", reforça Catarina Mascarenhas. Na prática, uma entidade crítica terá de cumprir ambos, através da montagem de um complexo *puzzle* regulatório que, em setores como o financeiro, inclui ainda uma terceira peça fundamental. "Importa salientar que no campo das entidades financeiras estas matérias, face ao princípio da especialidade, se encontram reguladas no DORA (Digital Operational Resilience Act)", acrescenta Catarina Mascarenhas.

PARA EMPRESAS DOS SETORES DA ENERGIA, TELECOMUNICAÇÕES E FINANCEIRO, "A ADAPTAÇÃO DESTAS ENTIDADES NÃO SERÁ NENHUM 'BICHO DE SETE CABEÇAS'", UMA VEZ QUE JÁ POSSUEM POLÍTICAS DE GESTÃO DE RISCO AVANÇADAS. "DE TODO O MODO, NÃO DEIXA DE SER MAIS UM DECRETO-LEI QUE AS ENTIDADES TERÃO DE ANALISAR, DOMINAR E ADAPTAR À SUA REALIDADE, O QUE APENAS REFORÇA A IMPORTÂNCIA REGULATÓRIA DA CIBERSEGURANÇA NO CONTEXTO ATUAL",

O PESO DAS SANÇÕES E A GOVERNANÇA DO RISCO

O incumprimento não será uma opção, uma vez que o legislador dotou o regime de um arsenal sancionatório desenvolvido para garantir a sua aplicação efetiva. José Maria Alves Pereira explica que, perante uma suspeita, o processo pode começar de forma pedagógica: "as entidades críticas poderão ser sujei-

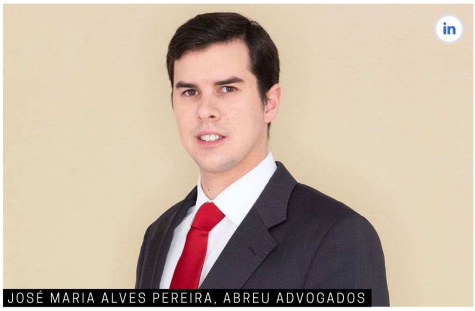
tas a advertências", contendo as normas infringidas e as medidas corretivas a implementar.

Contudo, a persistência na falha pode levar à "aplicação de coimas pelas infrações praticadas, além de sanções pecuniárias compulsórias enquanto se mantiver a infração".

Esta última ferramenta, em particular, pode representar um encargo financeiro contínuo e pesado para as organizações que adiem a conformidade. A fiscalização e aplicação destas sanções caberá ao Secretário-Geral do Sistema de Segurança Interna, solidificando a governança do regime.

DA RESILIÊNCIA À VANTAGEM COMPETITIVA EM SETORES SENSÍVEIS

Encarar este Decreto-Lei apenas como um fardo de conformidade é um erro estratégico, já que as empresas que abraçarem a resiliência como um pilar da sua operação podem colher benefícios significativos.


JOSÉ MARIA ALVES PEREIRA, ABREU ADVOGADOS

Pensemos no setor da energia. Um produtor ou distribuidor que demonstre, através de planos robustos e exercícios testados, a sua capacidade de manter o fornecimento durante uma crise – seja um ciberataque, uma falha de equipamento ou uma seca prolongada – não está apenas a cumprir a lei. Está a oferecer uma garantia de fiabilidade aos seus clientes industriais e a posicionar-se como um parceiro mais seguro nas cadeias de abastecimento europeias.

PERANTE UMA SUSPEITA, O PROCESSO PODE COMEÇAR DE FORMA PEDAGÓGICA: "AS ENTIDADES CRÍTICAS PODERÃO SER SUJEITAS A ADVERTÊNCIAS", CONTENDO AS NORMAS INFRINGIDAS E AS MEDIDAS CORRETIVAS A IMPLEMENTAR. CONTUDO, A PERSISTÊNCIA NA FALHA PODE LEVAR À "APLICAÇÃO DE COIMAS PELAS INFRAÇÕES PRATICADAS, ALÉM DE SANÇÕES PECUNIÁRIAS COMPULSÓRIAS ENQUANTO SE MANTIVER A INFRAÇÃO".