MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

DIRETIVA SRI2 (NIS2)

Enquadramento

A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (**SRI2** ou **Diretiva**), foi publicada no Jornal Oficial da União Europeia, a 27 de dezembro de 2022.

A SRI2 foi criada num contexto contemporâneo de urgência, perante a necessidade contínua e crescente de oferecer uma resposta mais sofisticada à frequência e complexidade das ciberameaças, com o propósito global de melhorar e fortalecer a cibersegurança e proteger as infraestruturas críticas em toda a União Europeia (**UE**).
A Diretiva em vigor baseia-se, fundamentalmente, na anterior SRI, abordando várias lacunas existentes e expandindo o seu âmbito de aplicação com o objetivo de aprimorar os requisitos de segurança, as obrigações de comunicação e as capacidades de gestão de crises e incidentes.

Entre as principais alterações e avanços, a SRI2 amplia significativamente o seu alcance, de modo a abranger uma gama mais vasta de setores e entidades e, paralelamente, *i)* estabelece obrigações de comunicação de incidentes mais rigorosas e objetivas, traduzidas num quadro unificado; *ii)* atribui maior ênfase à segurança da cadeia de abastecimento (*supply chain*); *iii)* aborda áreas de risco emergentes; *iv)* promove uma adequada gestão das vulnerabilidades; *v)* destaca a importância de ciber-higiene; *vi)* introduz a necessidade de análises e avaliações interpares, fomentando uma maior cooperação e colaboração entre os Estados-Membros; e *vii)* alarga o âmbito de aplicação, passando a incluir médias e grandes empresas de diferentes setores.

Âmbito de aplicação

A SRI2 aplica-se às entidades públicas ou privadas de um dos tipos referidos no anexo I ou II, que sejam consideradas médias empresas nos termos do artigo 2.º do anexo da Recomendação 2003/361/CE, ou que excedam os limiares relativos às médias empresas previstos no n.º 1 do referido artigo, e que prestem os seus serviços ou exerçam as suas atividades na UE.

Tipos de empresas	
Médias	**Grandes**
Empregam entre 50 e 249 trabalhadores; Volume de negócios anual até 50 000 000 €; ou Ativo líquido/balanço total anual até 43 000 000 €	Empregam 250 ou mais trabalhadores; Volume de negócios anual superior a 50 000 000 €; ou Ativo líquido/balanço total anual superior a 43 000 000 €

As entidades abrangidas são classificadas em **entidades essenciais** e **entidades importantes**, de acordo com o artigo 3.º da SRI2, refletindo a medida em que são fundamentais no que concerne ao seu setor ou ao tipo de serviço que prestam, bem como a sua dimensão.

Classificação das entidades	
Essenciais	**Importantes**
Setores/Serviços • Energia; • Transportes; • Bancário; • Infraestruturas do mercado financeiro; • Saúde; • Água potável; • Infraestruturas digitais; • Gestão de serviços TIC; • Administração pública; • Espacial.	**Setores/Serviços** • Postais e de estafeta; • Gestão de resíduos; • Produção, fabrico e distribuição de produtos químicos; • Produção, transformação e distribuição de produtos alimentares; • Indústria transformadora; • Prestadores de serviços digitais; • Investigação.

Requisitos principais da SRI2

Para as entidades abrangidas, a SRI2 prevê um leque de requisitos fundados em pilares-chave, segundo os quais as mesmas se devem pautar de forma a garantir uma conformidade transversal dos seus procedimentos com as previsões europeias. Devem, assim, as entidades abrangidas, ao abrigo do *Cyber Crisis Management Structure* (**CyCLONe**), rever, criar, estabelecer e/ou melhorar:

- Políticas de cibersegurança e práticas de gestão de riscos;
- Procedimentos de gestão de incidentes, incluindo obrigações de comunicação e planos de resposta;
- Planeamentos da prossecução das atividades para garantir a continuidade dos serviços críticos em caso de incidente cibernético;
- Medidas de segurança da cadeia de abastecimento (*supply chain*) para avaliar e garantir a segurança de fornecedores terceiros;
- Programas de formação e sensibilização aos seus colaboradores para promover as melhores práticas de cibersegurança;
- Práticas de gestão de ativos para identificar e proteger sistemas e ativos de informação críticos;
- Obrigações de comunicação às autoridades competentes e manter as capacidades de resposta a incidentes.

Sanções em caso de incumprimento dos requisitos

É ideal que as entidades abrangidas revisitem, reformulem e reforcem as suas obrigações, em conformidade com os requisitos da Diretiva. Caso não o façam, naturalmente, tal poderá resultar em coimas e sanções significativas.

No caso das **entidades essenciais**, as coimas poderão atingir 10 000 000 € ou 2% do volume de negócios global da entidade, consoante o valor mais elevado. Já para as **entidades importantes**, as coimas poderão atingir 7 000 000 € ou 1,4% do volume de negócios global, consoante o que for mais elevado.

Muito para além da natureza destas sanções, é dada às autoridades nacionais a possibilidade de

aplicar outras medidas e sanções por incumprimento da Diretiva. Entre elas, contam-se as ordens de suspensão ou restrição das atividades da entidade com vista à proteção da segurança das redes e dos sistemas de informação.

Tabela-resumo comparativa entre a SRI e a SRI2

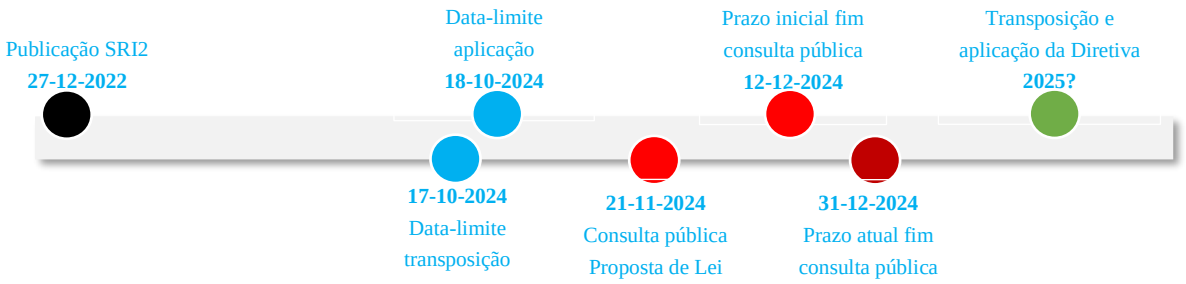
Tema	SRI	SRI2
Âmbito de aplicação	Aplica-se apenas a operadores de serviços essenciais em setores como energia, transportes, água e saúde, e a alguns prestadores de serviços digitais.	Alarga consideravelmente o âmbito, incluindo entidades médias e grandes em setores críticos como: • Administração pública; • Espaço; • Gestão de resíduos; • Químicos; • Produção e distribuição de alimentos; • Serviços postais e de correio expresso; • Fabrico de produtos críticos, como dispositivos médicos, eletrónica e maquinaria.
Nível de harmonização	Permite uma implementação flexível pelos Estados-Membros, resultando em requisitos de segurança e obrigações de reporte inconsistentes.	Harmoniza os requisitos de segurança e as obrigações de reporte entre os Estados-Membros, garantindo maior consistência.
***Governance* e supervisão**	Depende das autoridades nacionais para supervisão, com coordenação limitada a nível europeu.	Introduz coordenação a nível da UE através da Rede Europeia de Ligação para Crises Cibernéticas (EU-CyCLONe). Estabelece requisitos de governação mais rigorosos, incluindo a responsabilização ao nível da gestão das organizações.
Notificação de incidentes	As exigências de reporte são menos específicas, levando a práticas variadas entre os Estados-Membros.	Especifica prazos para reporte de incidentes: • Notificação inicial: dentro de 24 horas após a deteção: • Relatório final: dentro de um mês; • Clarifica o que constitui um “incidente significativo”.

Penalizações e Responsabilidade	As penalizações são determinadas pelos Estados-Membros, resultando em variações significativas.	Introduz penalizações mais rigorosas e uniformes. Destaca a responsabilidade ao nível da gestão, podendo os líderes enfrentar penalizações por não conformidade.
Riscos na cadeia de fornecimento e contratação de terceiros	Foco principal nas organizações abrangidas.	Dá maior ênfase à gestão de riscos na cadeia de fornecimento e de terceiros. Exige que as entidades avaliem e mitiguem os riscos associados a fornecedores e a prestadores de serviços.
Alocação de recursos e capacidades	Não exige explicitamente a alocação de recursos, com exceção do Responsável de Segurança.	Obriga as organizações a alocar recursos financeiros e humanos adequados para a cibersegurança.
Proatividade na cibersegurança	Foca-se essencialmente na resposta a incidentes.	Enfatiza a gestão de riscos proativa, incluindo: • Gestão de vulnerabilidades; • Monitorização contínua; • Práticas de resiliência cibernética.
Cooperação transfronteiriça	Depende de cooperação bilateral.	Reforça a cooperação a nível da UE. Formaliza o papel da ENISA (Agência da União Europeia para a Cibersegurança) no apoio aos Estados-Membros e às entidades.

A transposição da Diretiva SRI2 – O atual panorama português

A Diretiva SRI2 prevê que, até 17 de outubro de 2024, os Estados-Membros tivessem adotado as disposições necessárias com vista a dar cumprimento à Diretiva SRI2, aplicando-as a partir do dia seguinte, ou seja, 18 de outubro de 2024.

Embora já plenamente em vigor noutros ordenamentos jurídicos europeus, o contexto atual português é de incumprimento do Direito da UE, encontrando-se em curso o processo de transposição legislativa desta Diretiva, tendo sido a respetiva Proposta de Lei submetida a consulta pública apenas no dia 21 de novembro de 2024.



Encontra-se atualmente em vigor o Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018, de 13 de agosto), que transpôs a anterior Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, e que é complementado pelo Decreto-Lei n.º 65/2021, de 30 de julho, e pela Instrução Técnica do Centro Nacional de Cibersegurança aprovada pelo Regulamento n.º 183/2022. Naturalmente, a Proposta de Lei, ainda que ainda não tenha dado corpo a uma legislação de transposição, apresenta e estabelece, ao longo das suas 121 páginas, a exposição dos seus motivos, alterações e questões inalteráveis, tudo face ao regime atual.

Assim, sumariamente, eis o que se pode esperar, em linha com a SRI2: *i)* ampliação do número de entidades sujeitas; *ii)* medidas de gestão da avaliação de risco; *iii)* segurança da cadeia de abastecimento; *iv)* criação da Comissão de Avaliação da Segurança do Ciberespaço; *v)* imposição de restrições e cessação de utilização; *vi)* reforço e atualização da estratégia nacional de segurança do ciberespaço; *vii)* aprovação de um plano nacional de resposta a crises cibernéticas; *viii)* promoção da certificação em cibersegurança; *ix)* regime processual sancionatório.

Não serão objeto de alteração as questões relativas às obrigações de notificação de incidentes, à existência do Responsável pela Cibersegurança e do Ponto de Contacto Permanente e, ainda, do envio do Relatório Anual ao Centro Nacional de Cibersegurança (CNCS).

Logo que a transposição seja efetivada, as entidades abrangidas deverão, sob pena de sanções em virtude de incumprimento[1]:

- Proceder à sua autoidentificação, de acordo com a sua natureza, na plataforma eletrónica disponibilizada pelo CNCS, no prazo de um mês após o início da sua atividade;
- Proceder à sua autoidentificação, no prazo de 60 dias após a disponibilização da referida plataforma eletrónica, caso já se encontrem em atividade aquando da entrada em vigor do (futuro) Decreto-Lei;
- Manter, em qualquer caso, a informação devidamente atualizada.

Para maior detalhe sobre se a sua empresa estará sujeita a esta Diretiva e, ainda, como tais alterações podem ter um impacto na sua organização, entre em contacto com a nossa equipa.

David Silva Ramalho
Nicole Fortunato
Adriana Brás
Inês Costa Bastos
Ana Xavier Nunes

[1] Caso o procedimento de autoidentificação não seja cumprido adequada e temporaneamente, tal constituirá uma contraordenação grave, punível com coimas entre 1.250,00 € e 5.000.000,00 € ou 1% do volume de negócios anual mundial no exercício financeiro anterior, consoante o valor mais elevado, à luz do artigo 62.º da Proposta de Lei.