COMISSÃO
EUROPEIA

Bruxelas, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposta de

# DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO

## relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148

(Texto relevante para efeitos do EEE)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

# EXPOSIÇÃO DE MOTIVOS

## 1. CONTEXTO DA PROPOSTA

### • Razões e objetivos da proposta

A presente proposta faz parte de um pacote de medidas destinadas a melhorar a resiliência e a capacidade de resposta a incidentes no domínio da cibersegurança e da proteção de infraestruturas críticas por parte das entidades públicas e privadas, das autoridades competentes e da União no seu conjunto. É consentânea com as prioridades da Comissão no sentido de preparar a Europa para a era digital e criar uma economia pronta para o futuro e que esteja ao serviço dos cidadãos. A cibersegurança é uma das áreas prioritárias da resposta da Comissão à crise da COVID-19. O pacote inclui uma nova estratégia em matéria de cibersegurança, com o objetivo de reforçar a autonomia estratégia da União para melhorar a sua resiliência e a sua resposta coletiva, bem como para construir uma Internet aberta e global. Por último, o pacote contém uma proposta de diretiva relativa à resiliência de operadores críticos de serviços essenciais, que visa minimizar as ameaças físicas contra tais operadores.

A presente proposta tem por base e revoga a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação (Diretiva SRI), que constitui o primeiro ato legislativo à escala da União sobre cibersegurança e que estabelece medidas jurídicas para melhorar o nível geral de cibersegurança na União. A Diretiva SRI: 1) contribuiu para melhorar as capacidades de cibersegurança a nível nacional, exigindo que os Estados-Membros adotassem estratégias nacionais de cibersegurança e que designassem autoridades competentes neste domínio; 2) reforçou a cooperação entre os Estados-Membros a nível da União, criando vários fóruns para facilitar o intercâmbio de informações estratégicas e operacionais; 3) melhorou a ciber-resiliência de entidades públicas e privadas em sete setores específicos (energia, transportes, serviços bancários, infraestruturas do mercado financeiro, cuidados de saúde, fornecimento e distribuição de água potável, e infraestruturas digitais) e em três serviços digitais (mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem), exigindo que os Estados-Membros se certifiquem de que os operadores de serviços essenciais e os prestadores de serviços digitais estabelecem requisitos de cibersegurança e notificam incidentes.

A proposta moderniza o atual quadro jurídico, tendo em conta a crescente digitalização do mercado interno nos últimos anos e a evolução do cenário de ameaças à cibersegurança. Estes dois desenvolvimentos intensificaram-se desde o início da crise da COVID-19. A proposta aborda igualmente várias deficiências que impediram a Diretiva SRI de concretizar todo o seu potencial.

Não obstante ter produzido resultados dignos de nota, a Diretiva SRI, que abriu as portas a uma mudança significativa das mentalidades em relação à abordagem institucional e regulamentar à cibersegurança em muitos Estados-Membros, também revelou claramente as suas limitações. A transformação digital da sociedade (intensificada pela crise da COVID-19) alargou o cenário de ameaças e está a gerar novos desafios que requerem respostas adaptadas e inovadoras. O número de ciberataques continua a aumentar, com ataques cada vez mais sofisticados provenientes de uma grande variedade de fontes dentro e fora da UE.

A avaliação da aplicação da Diretiva SRI, realizada para efeitos da avaliação de impacto, identificou as seguintes questões problemáticas: 1) o baixo nível de ciber-resiliência das empresas que operam na UE; 2) as diferenças em termos de resiliência entre Estados-Membros e setores; 3) o baixo nível de conhecimento situacional comum e a inexistência de mecanismos de resposta conjunta a situações de crise. Por exemplo, alguns dos principais hospitais num Estado-Membro não estão abrangidos pelo âmbito da Diretiva

SRI e, como tal, não estão obrigados a aplicar as medidas de segurança nela previstas, ao passo que, noutro Estado-Membro, praticamente todos os prestadores de cuidados de saúde do país estão sujeitos aos requisitos de segurança estabelecidos nessa diretiva.

Sendo uma iniciativa lançada no âmbito do programa para a adequação e a eficácia da regulamentação (REFIT), a proposta visa reduzir os encargos regulamentares das autoridades competentes e os custos de conformidade suportados por entidades públicas e privadas. Este objetivo é alcançado, em especial, por via da eliminação da obrigação das autoridades competentes de identificarem operadores de serviços essenciais e de uma maior harmonização dos requisitos de segurança e de notificação, a fim de facilitar a conformidade regulamentar por parte das entidades que prestam serviços transfronteiriços. Simultaneamente, serão também atribuídas novas funções às autoridades competentes, incluindo a supervisão de entidades em setores que até agora não estavam abrangidos pela Diretiva SRI.

- **Coerência com as disposições existentes da mesma política setorial**

A presente proposta integra-se num conjunto mais amplo de instrumentos legais existentes e iniciativas programadas a nível da União, que visam aumentar a resiliência das entidades públicas e privadas contra ameaças.

No domínio da cibersegurança, importa destacar a Diretiva (UE) 2018/1972 que estabelece o Código Europeu das Comunicações Eletrónicas (cujas disposições relacionadas com a cibersegurança serão substituídas pelas disposições da presente proposta) e a proposta de regulamento relativo à resiliência operacional digital do setor financeiro [COM(2020) 595 final], que será considerado uma *lex specialis* em relação à presente proposta, após a entrada em vigor de ambos os atos.

No domínio da segurança física, a proposta completa a proposta de diretiva relativa à resiliência de entidades críticas, que revê a Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (Diretiva ICE), que estabelece um processo à escala da União para identificar e designar infraestruturas críticas europeias e define uma abordagem para melhorar a sua proteção. Em julho de 2020, a Comissão adotou a Estratégia da UE para a União da Segurança[1], que reconheceu a crescente interconexão e interdependência entre infraestruturas físicas e digitais. Além disso, sublinhou a necessidade de uma abordagem mais coerente e consistente entre a Diretiva ICE e a Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Por conseguinte, a proposta está estreitamente alinhada com a proposta de diretiva relativa à resiliência de entidades críticas, que visa reforçar a resiliência de entidades críticas contra ameaças físicas num grande número de setores. A proposta visa assegurar que as autoridades competentes ao abrigo dos dois atos jurídicos adotam medidas complementares e trocam as informações necessárias sobre ciber-resiliência e resiliência a outros níveis, e que os operadores particularmente críticos nos setores considerados «essenciais» de acordo com a presente proposta estão também sujeitos a obrigações mais gerais destinadas a reforçar a resiliência, com especial incidência nos riscos não relacionados com a cibersegurança.

[1] COM(2020) 605 final.

- **Coerência com outras políticas da União**

Tal como referido na Comunicação «Construir o futuro digital da Europa»[2], é crucial que a Europa tire partido de todos os benefícios da era digital e reforce a sua capacidade industrial e de inovação dentro de limites éticos e seguros. A estratégia europeia para os dados define quatro pilares — a proteção de dados, os direitos fundamentais, a segurança e a cibersegurança —, que constituem condições essenciais para uma sociedade capacitada pela utilização dos dados.

Numa Resolução de 12 de março de 2019, o Parlamento Europeu instou «[…] a Comissão a ponderar a necessidade de alargar o âmbito de aplicação da Diretiva SRI a novos setores e serviços críticos que não sejam abrangidos por legislação setorial»[3]. Nas suas Conclusões de 9 de junho de 2020, o Conselho congratulou-se com «[…] os planos da Comissão que visam garantir regras coerentes para os operadores de mercado e facilitar uma partilha de informações segura, sólida e adequada sobre ameaças e incidentes, nomeadamente através de uma revisão da Diretiva Segurança das Redes e da Informação (Diretiva SRI), a fim de encontrar soluções que melhorem a ciber-resiliência e de dar uma resposta mais eficaz aos ciberataques, em particular no contexto das atividades económicas e societais de caráter essencial, sem deixar de respeitar as competências dos Estados-Membros, incluindo a responsabilidade pela sua segurança nacional»[4]. Adicionalmente, o ato jurídico proposto não prejudica a aplicação das regras em matéria de concorrência estabelecidas no Tratado sobre o Funcionamento da União Europeia (TFUE).

Uma vez que uma parte significativa das ameaças à cibersegurança tem origem fora da UE, é necessária uma abordagem coerente à cooperação internacional. A presente diretiva constitui um modelo de referência a promover no contexto da cooperação da UE com países terceiros, especialmente no âmbito da prestação de assistência técnica externa.

## 2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

- **Base jurídica**

A base jurídica da Diretiva SRI é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, cujo objetivo consiste no estabelecimento e funcionamento do mercado interno por intermédio do reforço de medidas relativas à aproximação das regras nacionais. Tal como sustentou o Tribunal de Justiça da UE no Acórdão de 8 de junho de 2010 no processo C-58/08, Vodafone e o., o recurso ao artigo 114.º do TFUE é justificado em caso de divergências entre as regulamentações nacionais que tenham uma influência direta no funcionamento do mercado interno. Do mesmo modo, o Tribunal de Justiça entendeu que, quando um ato baseado no artigo 114.º do TFUE já eliminou todos os obstáculos às trocas comerciais no domínio que harmoniza, o legislador da União não pode ser privado da possibilidade de adaptar esse ato a qualquer alteração de circunstâncias ou a qualquer evolução dos conhecimentos, tendo em conta a missão que lhe incumbe de velar pela proteção dos interesses gerais reconhecidos pelo Tratado. Por último, o Tribunal de Justiça considerou que a expressão «medidas relativas à aproximação» que figura no artigo 114.º do TFUE se destina a conferir, em função do contexto geral e das circunstâncias específicas da matéria a harmonizar, uma margem de apreciação quanto à técnica de aproximação mais adequada para

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_PT.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/pt/pdf.

alcançar o resultado pretendido. O ato jurídico proposto eliminaria obstáculos ao mercado interno e melhoraria o seu estabelecimento e funcionamento para entidades essenciais e importantes, nomeadamente: estabelecendo regras claras de aplicação geral sobre o âmbito de aplicação da Diretiva SRI e harmonizando as regras aplicáveis no domínio da gestão dos riscos de cibersegurança e da notificação de incidentes. As disparidades existentes neste domínio, tanto a nível legislativo como de supervisão, assim como a nível nacional e da UE, constituem obstáculos ao mercado interno, uma vez que as entidades que exercem atividades transfronteiriças deparam-se com diferenças e, eventualmente, duplicações dos requisitos regulamentares e/ou da sua aplicação, as quais prejudicam o exercício da liberdade de estabelecimento e de prestação de serviços. As diferenças de regulamentação também afetam negativamente as condições de concorrência no mercado interno quando estão em causa entidades do mesmo tipo em Estados-Membros diferentes.

- **Subsidiariedade (no caso de competência não exclusiva)**

A ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de medidas nacionais ou regionais estanques. A Diretiva SRI responde, em parte, a este problema, visto que estabelece um quadro para a segurança das redes e dos sistemas de informação a nível nacional e da União. Porém, a sua transposição e aplicação revelaram também as deficiências e os limites intrínsecos de certas disposições ou abordagens, como o facto de a falta de clareza quanto à definição do âmbito da diretiva dar origem a diferenças significativas em termos de extensão e profundidade da intervenção efetiva da UE a nível dos Estados-Membros. Acresce que, desde o início da crise da COVID-19, a economia europeia está mais dependente do que nunca das redes e dos sistemas de informação e a interligação entre setores e serviços é cada vez maior. Uma intervenção da UE que vá além das atuais medidas previstas na Diretiva SRI justifica-se principalmente pelo: i) crescente caráter transfronteiriço das ameaças e dos desafios relacionados com SRI; ii) potencial da ação da União para melhorar a eficácia e facilitar a coordenação das políticas nacionais; iii) contributo de ações políticas concertadas e colaborativas para uma proteção eficaz dos dados e da privacidade.

- **Proporcionalidade**

As regras propostas na presente diretiva não excedem o necessário para atingir os objetivos específicos de forma satisfatória. A harmonização e simplificação previstas das medidas de segurança e das obrigações de notificação estão associadas a pedidos formulados pelos Estados-Membros e pelas empresas no sentido de melhorar o quadro atual.

A proposta tem em conta as práticas vigentes nos Estados-Membros. A imposição de requisitos simplificados e coordenados para melhorar o nível de proteção é proporcionada em relação aos riscos cada vez mais elevados que enfrentamos, incluindo aqueles que apresentam um elemento transfronteiriço; esses requisitos são razoáveis e, de um modo geral, correspondem ao interesse das entidades envolvidas em garantir a continuidade e a qualidade dos seus serviços. Os custos associados à garantia de uma cooperação sistemática entre os Estados-Membros seriam baixos em comparação com as perdas e os danos económicos e sociais causados por incidentes de cibersegurança. Além disso, as consultas das partes interessadas realizadas no contexto da avaliação da Diretiva SRI, incluindo os resultados da consulta pública aberta e de inquéritos específicos, revelam apoio à revisão da Diretiva SRI nos moldes supramencionados.

- **Escolha do instrumento**

A proposta simplificará as obrigações impostas às empresas e assegurará um nível mais elevado de harmonização das mesmas. Paralelamente, a proposta visa proporcionar aos Estados-Membros a flexibilidade necessária para terem em conta especificidades nacionais (tais como a possibilidade de identificar entidades essenciais ou importantes adicionais, não incluídas no conjunto de base definido no ato jurídico). Consequentemente, o futuro instrumento jurídico deverá ser uma diretiva, uma vez que permite melhorar e direcionar a harmonização, bem como conferir um certo grau de flexibilidade às autoridades competentes.

## 3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- **Avaliações *ex post*/balanços de qualidade da legislação existente**

A Comissão procedeu a uma avaliação da aplicação da Diretiva SRI[5], tendo analisado a sua pertinência, coerência, eficácia, eficiência e valor acrescentado da UE. As principais constatações desta análise são:

- O âmbito da Diretiva SRI é demasiado limitado em termos dos setores abrangidos, principalmente devido: i) ao aumento da digitalização nos últimos anos e a um maior grau de interligação, ii) ao facto de já não refletir todos os setores digitalizados que prestam serviços fundamentais à economia e à sociedade como um todo.
- A Diretiva SRI não é suficientemente clara no que respeita ao âmbito dos operadores de serviços essenciais e as suas disposições não definem com clareza suficiente a competência nacional em relação aos prestadores de serviços digitais. Tal criou uma situação em que certos tipos de entidades não foram identificadas em todos os Estados-Membros e, como tal, não estão obrigadas a adotar medidas de segurança e a notificar incidentes.
- A Diretiva SRI concedeu aos Estados-Membros uma ampla margem de apreciação no estabelecimento dos requisitos em matéria de segurança e de notificação de incidentes aplicáveis aos operadores de serviços essenciais (a seguir designados por «OSE»). A avaliação revela que, em alguns casos, os Estados-Membros aplicaram estes requisitos de formas muito díspares, criando encargos adicionais para as empresas que operam em mais do que um Estado-Membro.
- O regime de supervisão e execução coerciva da Diretiva SRI é ineficaz. Por exemplo, os Estados-Membros têm mostrado grande relutância em aplicar sanções às entidades que não estabeleçam requisitos de segurança ou que não notifiquem incidentes. Esta situação pode ter consequências negativas para a ciber-resiliência de entidades individuais.
- Os recursos financeiros e humanos afetados pelos Estados-Membros ao desempenho das suas funções (tais como a identificação ou a supervisão de OSE) e, consequentemente, os níveis de maturidade na gestão de riscos de cibersegurança variam muito. Esta divergência acentua ainda mais as diferenças entre o grau de ciber-resiliência dos Estados-Membros.
- O facto de os Estados-Membros não partilharem sistematicamente informações entre si tem consequências negativas, sobretudo para a eficácia das medidas de

[5] [Anexo 5 da avaliação de impacto].

cibersegurança e para o nível de conhecimento situacional comum à escala da UE. Tal é igualmente válido para a partilha de informações entre entidades privadas e para a relação entre as estruturas de cooperação a nível da UE e as entidades privadas.

- **Consultas das partes interessadas**

A Comissão consultou um vasto leque de partes interessadas. Os Estados-Membros e as partes interessadas foram convidadas a participar na consulta pública aberta e nos inquéritos e nas sessões de trabalho organizadas pela Wavestone, pelo CEPE e pela ICF, que a Comissão contratou para a realização de um estudo de apoio à avaliação da Diretiva SRI. Entre as partes interessadas figuravam autoridades competentes, organismos da União responsáveis por questões de cibersegurança, operadores de serviços essenciais, prestadores de serviços digitais, entidades que prestam serviços não abrangidos pelo âmbito da atual Diretiva SRI, associações comerciais, organizações de consumidores e cidadãos.

Além disso, a Comissão tem estado em contacto permanente com as autoridades competentes encarregadas de dar execução à Diretiva SRI. O grupo de coordenação cobriu exaustivamente vários aspetos transversais e setoriais da execução. Por último, durante as visitas realizadas aos países em 2019 e 2020 no âmbito da Diretiva SRI, a Comissão entrevistou 154 entidades públicas e privadas, bem como 117 autoridades competentes.

- **Recolha e utilização de conhecimentos especializados**

A Comissão contratou um consórcio constituído pela Wavestone, pelo CEPE e pela ICF para a apoiar na avaliação da Diretiva SRI[6]. Além de ter contactado as partes interessadas diretamente afetadas pela Diretiva SRI por meio de inquéritos específicos e sessões de trabalho, o consórcio contratado consultou igualmente um vasto leque de peritos no domínio da cibersegurança, tais como investigadores e profissionais da indústria de cibersegurança.

- **Avaliação de impacto**

A presente proposta é acompanhada por uma avaliação de impacto[7], que foi apresentada ao Comité de Controlo da Regulamentação (CCR) em 23 de outubro de 2020, tendo recebido um parecer favorável, com observações, em 20 de novembro de 2020. O CCR recomendou que fossem feitas melhorias em algumas áreas, com vista a: 1) refletir melhor o papel das repercussões transfronteiriças na análise do problema; 2) explicar melhor em que se traduziria o sucesso da iniciativa; 3) justificar mais detalhadamente a lista de opções políticas; 4) esclarecer melhor os custos das medidas propostas. A avaliação de impacto foi ajustada para ter em conta estas questões, bem como observações mais pormenorizadas formuladas pelo CCR. Como tal, inclui agora explicações mais detalhadas sobre o papel das repercussões transfronteiriças no domínio da cibersegurança, uma descrição mais clara da forma como o sucesso pode ser aferido, uma explicação mais detalhada da conceção e da lógica subjacente às diferentes opções políticas e às medidas contempladas no âmbito dessas opções, uma explicação mais detalhada dos aspetos analisados em relação ao âmbito setorial da Diretiva SRI e clarificações adicionais em matéria de custos.

---

6 Wavestone, CEPS e ICF, *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)* — n.º 2020-665.

7 **[Inserir ligações para o documento final e para a ficha de síntese.]**

A Comissão ponderou um conjunto de opções políticas para melhorar o quadro jurídico no domínio da ciber-resiliência e da resposta a incidentes:

- Manutenção do *status quo*: A Diretiva SRI não seria alterada e não seriam adotadas quaisquer outras medidas de natureza não legislativa para resolver os problemas identificados pela avaliação da referida diretiva.
- Opção 1: Não seriam introduzidas quaisquer alterações a nível legislativo. Em vez disso, a Comissão emitiria recomendações e orientações (nomeadamente em matéria de identificação de operadores de serviços essenciais, requisitos de segurança, procedimentos de notificação de incidentes e supervisão), após consulta do grupo de coordenação, da Agência da UE para a Cibersegurança (ENISA) e, se pertinente, da rede de equipas de resposta a incidentes de segurança informática (CSIRT).
- Opção 2: Esta opção implica a introdução de alterações específicas na Diretiva SRI, incluindo um alargamento do seu âmbito, e muitas outras alterações que teriam por objetivo garantir certas soluções imediatas para os problemas identificados, proporcionando mais clareza e maior harmonização (tais como disposições para harmonizar os limites de identificação). No entanto, a Diretiva SRI alterada manteria os seus principais elementos constituintes, a sua abordagem e a sua fundamentação lógica.
- Opção 3: Este cenário implica alterações sistémicas e estruturais da Diretiva SRI (introduzidas por uma nova diretiva) que visam uma mudança mais profunda da abordagem adotada até agora no sentido de abranger um segmento mais alargado das economias da União, mas com uma supervisão mais direcionada para grandes operadores e operadores fundamentais. Permite igualmente simplificar as obrigações impostas às empresas e assegurar um nível mais elevado de harmonização das mesmas, criar um quadro mais eficaz para os aspetos operacionais, bem como estabelecer uma base clara para reforçar as responsabilidades partilhadas e a responsabilização das várias partes interessadas em relação a medidas de cibersegurança.

A avaliação de impacto levou à conclusão de que a opção 3 é a preferida (ou seja, alterações sistémicas e estruturais do quadro para a SRI). Em termos de eficácia, a opção preferida determinaria claramente o âmbito da Diretiva SRI, que seria alargado a um segmento mais representativo das economias e sociedades da UE, e permitiria simplificar os requisitos, bem como definir melhor o quadro de supervisão e execução coerciva com o objetivo de aumentar o nível de conformidade. Implicaria ainda a adoção de medidas destinadas a melhorar as abordagens ao desenvolvimento de políticas a nível dos Estados-Membros e a mudar o respetivo paradigma, bem como a promover novos quadros de gestão dos riscos associados às relações com os fornecedores e uma divulgação coordenada de vulnerabilidades. Paralelamente, a opção política preferida estabeleceria uma base clara para a partilha de responsabilidades e a responsabilização e preveria mecanismos destinados a fomentar a confiança entre os Estados-Membros, tanto a nível das autoridades como da indústria, incentivando a partilha de informações e garantido uma abordagem mais operacional, como a assistência mútua e os mecanismos de análise pelos pares. Esta opção também proporcionaria um quadro para a gestão de crises a nível da UE, com base na rede operacional da UE lançada recentemente, e asseguraria um maior envolvimento da ENISA, no âmbito do seu atual mandato, na formação de uma panorâmica fiel do estado da cibersegurança na União.

Em termos de eficiência, embora a opção preferida implique custos adicionais em matéria de conformidade e de execução coerciva para as empresas e os Estados-Membros, conduziria

também a sinergias e soluções de compromissos eficientes, sendo os potenciais benefícios de todas as opções políticas analisados para garantir um nível acrescido e consistente de ciber-resiliência das entidades fundamentais em toda a União, o que acabaria por conduzir a uma redução dos custos, tanto para as empresas como para a sociedade. Esta opção política criaria certos encargos administrativos e custos de conformidade adicionais para as autoridades dos Estados-Membros. Porém, de um modo geral, a médio e a longo prazo, traria igualmente benefícios substanciais graças a uma cooperação acrescida entre os Estados-Membros, nomeadamente a nível operacional, e incentivaria um reforço global das capacidades de cibersegurança a nível nacional e regional, por via da assistência mútua, do estabelecimento de mecanismos de análise pelos partes e de uma panorâmica mais informada das empresas-chave, bem como de uma maior interação com estas. A opção política preferida asseguraria também, em larga medida, a coerência com outros atos legislativos, iniciativas e medidas políticas, nomeadamente com *lex specialis* adotada a nível setorial.

A resolução do atual problema da insuficiente preparação no domínio da cibersegurança a nível dos Estados-Membros e das empresas e de outras organizações poderia originar ganhos de eficiência e a redução de custos adicionais resultantes de incidentes de cibersegurança.

- Para as entidades essenciais e importantes, o aumento do nível de preparação no domínio da cibersegurança poderia levar à minimização de potenciais perdas de receitas devido a perturbações (incluindo as resultantes de espionagem industrial) e reduzir as elevadas despesas decorrentes de medidas *ad hoc* de atenuação das ameaças. É provável que tais benefícios compensem os necessários custos de investimento. A redução da fragmentação no mercado interno criaria também condições de concorrência mais equitativas entre os operadores.
- Para os Estados-Membros, poderia reduzir ainda mais o risco de aumento das despesas orçamentais com medidas *ad hoc* de atenuação das ameaças e de custos adicionais em caso de emergências relacionadas com incidentes de cibersegurança.
- Para os cidadãos, espera-se que a resposta a incidentes de cibersegurança faça diminuir as perdas de rendimento decorrentes de perturbações económicas.

O aumento dos níveis de cibersegurança nos Estados-Membros e a capacidade de as empresas e as autoridades responderem rapidamente a um incidente e atenuarem o seu impacto conduzirá muito provavelmente a um reforço da confiança geral dos cidadãos na economia digital, o que poderá ter um impacto positivo no crescimento e no investimento.

O aumento do nível global de cibersegurança é suscetível de conduzir a um aumento da segurança global e ao funcionamento ininterrupto e harmonioso de serviços essenciais, que são de importância crítica para a sociedade. A iniciativa poderá também contribuir para outros impactos sociais, como a redução dos níveis de cibercriminalidade e de terrorismo e o reforço da proteção civil. Quanto mais preparadas estiverem as empresas e outras organizações em matéria de cibersegurança, maiores serão as probabilidades de evitar potenciais perdas financeiras decorrentes de ciberataques e, consequentemente, de evitar despedimentos.

O aumento do nível global de cibersegurança poderia ainda contribuir para a prevenção de riscos/danos ambientais em caso de ataque a um serviço essencial, sobretudo nos setores da energia, do fornecimento e distribuição de água e dos transportes. Ao reforçar as capacidades de cibersegurança, a iniciativa poderia conduzir a uma maior utilização de infraestruturas e serviços de TIC de última geração, que são também mais sustentáveis do ponto de vista ambiental, e à substituição de infraestruturas pré-existentes ineficientes e menos seguras. Tal

deverá contribuir igualmente para reduzir o número de ciberincidentes dispendiosos, libertando recursos para investimentos sustentáveis.

- **Adequação da regulamentação e simplificação**

A proposta prevê a exclusão geral de micro e pequenas entidades do âmbito da Diretiva SRI e a aplicação de um regime de supervisão *ex post* mais simples a um vasto número de entidades que passam a estar abrangidas pelo âmbito de aplicação revisto (as chamadas «entidades importantes»). Estas medidas visam minimizar e equilibrar os encargos impostos às empresas e às administrações públicas. Adicionalmente, a proposta substitui o complexo sistema de identificação de operadores de serviços essenciais por uma obrigação de aplicação geral e introduz um nível mais elevado de harmonização das obrigações em matéria de segurança e de notificação, o que diminuiria os encargos de conformidade, especialmente para as entidades que prestam serviços transfronteiriços.

A proposta minimiza os custos de conformidade para as PME, uma vez que as entidades só são obrigadas a tomar as medidas necessárias para garantir um nível de segurança das redes e dos sistemas de informações consentâneo com os riscos que se colocam.

- **Direitos fundamentais**

A UE está empenhada em assegurar elevados níveis de proteção dos direitos fundamentais. Todos os acordos de partilha de informações a título voluntário entre entidades que esta diretiva promove seriam aplicados em ambientes de confiança, no pleno respeito das regras da União em matéria de proteção de dados, especialmente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[8].

## 4. INCIDÊNCIA ORÇAMENTAL

*Consultar ficha financeira*

## 5. OUTROS ELEMENTOS

- **Planos de execução e acompanhamento, avaliação e prestação de informações**

A proposta inclui um plano geral de acompanhamento e avaliação do impacto nos objetivos específicos, que exige que a Comissão proceda a uma avaliação, pelo menos, [54 meses] após a data de entrada em vigor e que preste informações ao Parlamento Europeu e ao Conselho sobre as suas principais constatações.

A avaliação deve ser realizada em conformidade com as Orientações «Legislar Melhor» da Comissão.

- **Explicação pormenorizada das disposições específicas da proposta**

A proposta está estruturada em torno de várias políticas setoriais importantes, que estão interligadas e que têm por objetivo aumentar o nível de cibersegurança na União.

[8] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

Objeto e âmbito (artigo 1.º e artigo 2.º)

Em particular, a diretiva: a) estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de cibersegurança e designarem autoridades nacionais competentes, pontos de contacto únicos e CSIRT; b) dispõe que os Estados-Membros devem impor obrigações de gestão dos riscos de cibersegurança e de notificação às entidades qualificadas como entidades essenciais no anexo I e como entidades importantes no anexo II; c) estabelece que os Estados-Membros devem impor obrigações em matéria de partilha de informações sobre cibersegurança.

A diretiva é aplicável a certas entidades essenciais, públicas ou privadas, que operam nos setores enumerados no anexo I (energia; transportes; serviços bancários; infraestruturas do mercado financeiro; saúde, água potável; águas residuais; infraestruturas digitais; administração pública e espaço) e a certas entidades importantes que operam nos setores enumerados no anexo II (serviços postais e de estafeta; gestão de resíduos; fabrico, produção e distribuição de produtos químicos; produção, transformação e distribuição de produtos alimentares; indústria transformadora e prestadores de serviços digitais). As micro e pequenas entidades, na aceção da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, estão excluídas do âmbito da diretiva, exceto os fornecedores de redes de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público, os prestadores de serviços de confiança, os registos de nomes de domínio de topo, a administração pública e certas outras entidades, tais como o único prestador de um serviço num Estado-Membro.

Quadros nacionais de cibersegurança (artigos 5.º a 11.º)

Os Estados-Membros devem adotar uma estratégia nacional de cibersegurança que defina objetivos estratégicos e medidas políticas e regulamentares adequadas, com vista a alcançar e a manter um elevado nível de cibersegurança.

A diretiva também estabelece um quadro para a divulgação coordenada de vulnerabilidades e exige que os Estados-Membros designem CSIRT para atuarem como intermediários de confiança e facilitarem a interação entre as entidades notificadoras e os fabricantes ou fornecedores de produtos de TIC e os prestadores de serviços de TIC. A ENISA deve criar e manter um registo europeu de vulnerabilidades detetadas.

Os Estados-Membros devem estabelecer quadros nacionais de gestão de crises de cibersegurança, nomeadamente designando autoridades nacionais competentes que sejam responsáveis pela gestão de incidentes e crises de cibersegurança em grande escala.

Os Estados-Membros devem igualmente designar uma ou várias autoridades nacionais competentes no domínio da cibersegurança para o exercício das funções de supervisão previstas na presente diretiva e um ponto de contacto único nacional em matéria de cibersegurança para desempenhar uma função de ligação com vista a assegurar a cooperação transfronteiriça das autoridades dos Estados-Membros. Devem ainda designar CSIRT.

Cooperação (artigos 12.º a 16.º)

A diretiva estabelece um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e de desenvolver a confiança entre os mesmos. Cria também uma rede de CSIRT que visa contribuir para o

desenvolvimento da confiança entre os Estados-Membros e para promover uma cooperação operacional célere e eficaz.

É criada uma Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe) para apoiar a gestão coordenada de incidentes e crises de cibersegurança em grande escala e para assegurar o intercâmbio regular de informações entre os Estados-Membros e as instituições da UE.

A ENISA deve elaborar, em cooperação com a Comissão, um relatório bienal sobre o estado da cibersegurança na União.

A Comissão deve estabelecer um sistema de análise pelos pares que permita analisar regularmente a eficácia das políticas de cibersegurança dos Estados-Membros.

Obrigações de gestão dos riscos de cibersegurança e de notificação (artigos 17.º a 23.º)

A diretiva exige que os Estados-Membros imponham aos órgãos de direção de todas as entidades abrangidas pelo seu âmbito a obrigação de aprovarem as medidas de gestão dos riscos de cibersegurança tomadas pelas respetivas entidades e de frequentarem ações de formação específicas no domínio da cibersegurança.

Os Estados-Membros devem assegurar que as entidades abrangidas pelo âmbito da diretiva tomem medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos de cibersegurança que se colocam à segurança das redes e dos sistemas de informação. Devem ainda garantir que as entidades notificam as autoridades nacionais competentes ou as CSIRT de qualquer incidente de cibersegurança que tenha um impacto significativo na prestação do serviço que asseguram.

Os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem recolher e manter dados exatos e completos relativos ao registo de nomes de domínio. Além disso, as referidas entidades devem proporcionar um acesso eficiente a dados relativos ao registo de nomes de domínio aos requerentes legítimos de acesso.

Competência e registo (artigos 24.º e 25.º)

Em regra, considera-se que as entidades essenciais e importantes estão sob a jurisdição do Estado-Membro onde prestam os seus serviços. No entanto, considera-se que certos tipos de entidades (prestadores de serviços de DNS, registos de nomes de domínio de topo, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados e fornecedores de redes de distribuição de conteúdos, bem como certos prestadores de serviços digitais) estão sob a jurisdição do Estado-Membro onde têm o seu estabelecimento principal na União. Pretende-se assim evitar que as referidas entidades estejam sujeitas a uma multiplicidade de requisitos legais, dado que uma proporção extremamente elevada dos serviços que prestam tem caráter transfronteiriço. A ENISA deve criar e manter um registo deste último tipo de entidades.

Partilha de informações (artigos 26.º e 27.º)

Os Estados-Membros devem estabelecer regras que permitam às entidades partilhar informações relacionadas com cibersegurança no quadro de acordos específicos de partilha de informações sobre cibersegurança, em conformidade com o artigo 101.º do TFUE. Além

disso, os Estados-Membros devem permitir que as entidades não abrangidas pelo âmbito da presente diretiva notifiquem, a título voluntário, incidentes significativos, ciberameaças ou quase incidentes.

Supervisão e execução coerciva (artigos 28.º a 34.º)

As autoridades competentes devem supervisionar as entidades abrangidas pelo âmbito da diretiva, devendo, nomeadamente, garantir que cumprem os requisitos em matéria de segurança e de notificação de incidentes. A diretiva distingue entre um regime de supervisão *ex ante* para as entidades essenciais e um regime de supervisão *ex post* para as entidades importantes; este último regime exige que as autoridades competentes intervenham quando disponham de provas ou indícios de que uma entidade importante não cumpre os requisitos em matéria de segurança e de notificação de incidentes.

A diretiva exige igualmente que os Estados-Membros imponham coimas às entidades essenciais e importantes e define coimas máximas.

Os Estados-Membros devem cooperar e assistir-se mutuamente, consoante necessário, quando as entidades prestam serviços em mais do que um Estado-Membros ou quando o estabelecimento principal de uma entidade ou o seu representante está localizado num determinado Estado-Membro, mas a sua rede e os seus sistemas de informação estão localizados em um ou vários Estados-Membros diferentes.

2020/0359 (COD)

Proposta de

# DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO

## relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[9],

Tendo em conta o parecer do Comité das Regiões[10],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[11] tinha por objetivo desenvolver as capacidades de cibersegurança em toda a União, atenuar as ameaças às redes e aos sistemas de informação utilizados para prestar serviços essenciais em setores-chave e garantir a continuidade de tais serviços em face de incidentes de cibersegurança, contribuindo assim para o eficaz funcionamento da economia e da sociedade da União.

(2) Desde a entrada em vigor da Diretiva (UE) 2016/1148, foram alcançados progressos significativos no sentido de aumentar a resiliência em matéria da cibersegurança da União. A avaliação dessa diretiva revelou que esta funcionou como um catalisador para a abordagem institucional e regulamentar à cibersegurança na União, abrindo as portas a uma mudança significativa das mentalidades. A referida diretiva assegurou a conclusão de quadros nacionais, mediante a definição de estratégias nacionais de cibersegurança, o estabelecimento de capacidades nacionais e a aplicação de medidas regulamentares que abrangem os intervenientes e as infraestruturas essenciais identificadas por cada Estado-Membro. Contribuiu igualmente para a cooperação a nível da União por via da criação do grupo de cooperação[12] e de uma rede de equipas nacionais de resposta a incidentes de segurança informática (a seguir designada por

9 JO C [...] de [...], p. [...].

10 JO C [...] de [...], p. [...].

11 Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194/1 de 19.7.2016, p. 1).

12 Artigo 11.º da Diretiva (UE) 2016/1148.

«rede de CSIRT»)[13]. Não obstante esses resultados, a avaliação da Diretiva (UE) 2016/1148 revelou deficiências intrínsecas que a impedem de responder de forma eficaz a desafios contemporâneos e emergentes no domínio da cibersegurança.

(3) Com a rápida transformação digital e interligação da sociedade, nomeadamente nos intercâmbios transfronteiriços, as redes e os sistemas de informação passaram a ocupar um lugar central na vida quotidiana. Essa evolução originou um alargamento do cenário de ameaças à cibersegurança, criando novos desafios que exigem respostas adaptadas, coordenadas e inovadoras em todos os Estados-Membros. O número, a amplitude, a sofisticação, a frequência e o impacto dos incidentes de cibersegurança estão a aumentar e constituem uma grave ameaça ao funcionamento das redes e dos sistemas de informação. Consequentemente, os ciberincidentes podem impedir o exercício de atividades económicas no mercado interno, gerar perdas financeiras, minar a confiança dos utilizadores e causar graves prejuízos à economia e à sociedade da União. Por conseguinte, a preparação e a eficácia no domínio da cibersegurança nunca foram tão importantes para o bom funcionamento do mercado interno como agora.

(4) A base jurídica da Diretiva (UE) 2016/1148 é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), cujo objetivo consiste no estabelecimento e funcionamento do mercado interno por intermédio do reforço de medidas relativas à aproximação das regras nacionais. Os requisitos de cibersegurança impostos às entidades que prestam serviços ou que exercem atividades economicamente importantes variam consideravelmente entre os Estados-Membros em termos do tipo de requisito, do seu grau de pormenor e do método de supervisão. Essas disparidades implicam custos adicionais e criam dificuldades para as empresas que propõem bens ou serviços além-fronteiras. As diferenças ou até mesmo as contradições entre os requisitos impostos por dois Estados-Membros podem afetar substancialmente essas atividades transfronteiriças. Além disso, as eventuais deficiências na conceção ou aplicação de normas de cibersegurança num Estado-Membro terão, provavelmente, repercussões no nível de cibersegurança de outros Estados-Membros, sobretudo em virtude dos intensos intercâmbios transfronteiriços. A avaliação da Diretiva (UE) 2016/1148 revelou grandes divergências na sua aplicação pelos Estados-Membros, nomeadamente em relação ao seu âmbito, cuja delimitação foi deixada, em larga medida, ao critério dos Estados-Membros. A Diretiva (UE) 2016/1148 também concedeu aos Estados-Membros uma margem de apreciação muito ampla relativamente à aplicação das obrigações nela estabelecidas em matéria de segurança e de notificação de incidentes. Tais obrigações foram, portanto, aplicadas de formas significativamente diferentes a nível nacional. Verificou-se uma divergência semelhante em relação às disposições dessa diretiva em matéria de supervisão e execução coerciva.

(5) Todas essas divergências implicam uma fragmentação do mercado interno e são suscetíveis de prejudicar o seu funcionamento, afetando, em especial, a prestação transfronteiriça de serviços e o nível de resiliência em matéria de cibersegurança devido à aplicação de normas diferentes. A presente diretiva visa eliminar essas divergências tão profundas entre os Estados-Membros, em especial estabelecendo regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado,

[13] Artigo 12.º da Diretiva (UE) 2016/1148.

criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações. Por conseguinte, a Diretiva (UE) 2016/1148 deve ser revogada e substituída pela presente diretiva.

(6) A presente diretiva não afeta a possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos interesses essenciais da sua própria segurança, salvaguardar a ordem e a segurança públicas e permitir a investigação, a deteção e a repressão de infrações penais, em conformidade com o direito da União. Nos termos do artigo 346.º do TFUE, nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação seria contrária aos interesses essenciais da sua segurança pública. São pertinentes neste contexto as regras nacionais e da União relativas à proteção de informações classificadas, os acordos de não divulgação e os acordos de não divulgação informais, tais como o protocolo «sinalização luminosa» (*Traffic Light Protocol*)[14].

(7) Com a revogação da Diretiva (UE) 2016/1148, o âmbito de aplicação por setor deve ser alargado a uma parte mais vasta da economia à luz dos aspetos referidos nos considerandos 4 a 6. Por conseguinte, é necessário alargar os setores abrangidos pela Diretiva (UE) 2016/1148, a fim de assegurar uma cobertura exaustiva dos setores e serviços de importância vital para as atividades económicas e sociais fundamentais no mercado interno. As regras não podem ser diferentes consoante as entidades sejam operadores de serviços essenciais ou prestadores de serviços digitais. Essa diferenciação revelou-se obsoleta, uma vez que não reflete a real importância dos setores ou serviços para as atividades económicas e sociais no mercado interno.

(8) Nos termos da Diretiva (UE) 2016/1148, cabia aos Estados-Membros determinar as entidades que cumpriam os critérios de classificação como operadores de serviços essenciais (a seguir designado por «processo de identificação»). A fim de eliminar as profundas divergências entre os Estados-Membros nesse domínio e proporcionar a todas as entidades jurídicas pertinentes segurança jurídica no que respeita aos requisitos de gestão de riscos e às obrigações de notificação, há que estabelecer um critério uniforme para identificar as entidades abrangidas pelo âmbito da presente diretiva. Tal critério deve consistir na aplicação da regra da limitação com base na dimensão da empresa, nos termos da qual todas as médias e grandes empresas, na aceção da Recomendação 2003/361/CE da Comissão[15], que atuam nos setores ou prestam o tipo de serviços abrangidos pela presente diretiva estão abrangidas pelo seu âmbito. Não deve ser exigido aos Estados-Membros que elaborem uma lista das entidades que cumprem este critério de aplicação geral relacionado com a dimensão.

(9) No entanto, as micro ou pequenas entidades que preencham certos critérios que indiciem o desempenho de um papel fundamental para as economias ou sociedades dos Estados-Membros ou para setores ou tipos de serviços específicos devem também estar abrangidas pela presente diretiva. Os Estados-Membros devem ser incumbidos de elaborar uma lista de tais entidades e apresentá-la à Comissão.

---

[14] O protocolo «sinalização luminosa» é um instrumento que permite a uma pessoa que partilha informações advertir os destinatários sobre possíveis limitações à disseminação posterior das mesmas. É utilizado em quase todas as comunidades de CSIRT e em alguns centros de partilha e análise de informações.

[15] Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

(10) Em cooperação com o grupo de cooperação, a Comissão pode emitir orientações sobre a aplicação dos critérios relativos às micro e pequenas empresas.

(11) Consoante o setor em que atuam ou o tipo de serviço que prestam, as entidades abrangidas pelo âmbito da presente diretiva devem ser classificadas em duas categorias: essenciais e importantes. Essa classificação deve ter em conta o grau de importância do setor ou do tipo de serviço, bem como o nível de dependência de outros setores ou tipos de serviços. Tanto as entidades essenciais como as entidades importantes devem estar sujeitas aos mesmos requisitos de gestão de riscos e obrigações de notificação. Os regimes de supervisão e de sanções aplicáveis a estas duas categorias devem ser diferentes, a fim de garantir um equilíbrio justo entre requisitos e obrigações, por um lado, e os encargos administrativos decorrentes da supervisão do cumprimento, por outro.

(12) A legislação e os instrumentos setoriais podem contribuir para assegurar elevados níveis de cibersegurança, tomando simultaneamente em plena consideração as especificidades e complexidades dos setores em causa. Nos casos em que um ato jurídico setorial da União exija que entidades essenciais ou importantes adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes ou ciberameaças significativas com, pelo menos, um efeito equivalente ao das obrigações estabelecidas na presente diretiva, devem aplicar-se essas disposições setoriais, nomeadamente em matéria de supervisão e execução coerciva. A Comissão pode emitir orientações relativas à aplicação da *lex specialis*. A presente diretiva não obsta à adoção de outros atos setoriais da União relacionados com medidas de gestão dos riscos de cibersegurança e notificação de incidentes. A presente diretiva não prejudica as atuais competências de execução atribuídas à Comissão em vários setores, incluindo transportes e energia.

(13) O Regulamento XXXX/XXXX do Parlamento Europeu e do Conselho[16] deve ser considerado um ato jurídico setorial da União para efeitos da presente diretiva no que diz respeito às entidades do setor financeiro. As disposições do Regulamento XXXX/XXXX relativas às medidas de gestão dos riscos no domínio das tecnologias da informação e comunicação (TIC), à gestão de incidentes relacionados com TIC e, em especial, à notificação de incidentes, bem como as relativas a testes de resiliência operacional digital, acordos de partilha de informações e riscos de terceiros no domínio das TIC, devem ser aplicadas em vez das disposições estabelecidas na presente diretiva. Por conseguinte, os Estados-Membros não devem aplicar as disposições da presente diretiva em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, partilha de informações e supervisão e execução coerciva no respeitante às entidades financeiras abrangidas pelo Regulamento XXXX/XXXX. Ao mesmo tempo, é importante manter uma relação sólida e o intercâmbio de informações com o setor financeiro no âmbito da presente diretiva. Para o efeito, o Regulamento XXXX/XXXX permite que todos os supervisores financeiros, as autoridades europeias de supervisão (AES) do setor financeiro e as autoridades nacionais competentes ao abrigo do Regulamento XXXX/XXXX participem nos debates políticos estratégicos e nos trabalhos técnicos do grupo de cooperação, e que troquem informações e cooperem com os pontos de contacto únicos designados nos termos da presente diretiva e com as CSIRT nacionais. As autoridades competentes ao abrigo do Regulamento XXXX/XXXX também devem transmitir

[16] *[Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos]*.

informações pormenorizadas sobre incidentes graves relacionados com as TIC aos pontos de contacto únicos designados nos termos da presente diretiva. Adicionalmente, os Estados-Membros devem continuar a incluir o setor financeiro nas respetivas estratégias de cibersegurança e as CSIRT nacionais podem contemplar o setor financeiro nas suas atividades.

(14) Tendo em conta as interligações entre a cibersegurança e a segurança física das entidades, importa assegurar uma abordagem coerente entre a Diretiva (UE) XXX/XXX do Parlamento Europeu e do Conselho[17] e a presente diretiva. Para tal, os Estados-Membros devem assegurar que as entidades críticas e as entidades equivalentes nos termos da Diretiva (UE) XXX/XXX sejam consideradas entidades essenciais no âmbito da presente diretiva. Os Estados-Membros devem ainda garantir que as suas estratégias de cibersegurança prevejam um quadro político para o reforço da cooperação entre a autoridade competente ao abrigo da presente diretiva e a autoridade competente ao abrigo da Diretiva (UE) XXX/XXX no contexto da partilha de informações sobre incidentes e ciberameaças e do exercício de funções de supervisão. As autoridades referidas nas duas diretivas devem cooperar e trocar informações, especialmente no que respeita à identificação de entidades críticas, ciberameaças, riscos de cibersegurança e incidentes que afetem entidades críticas, bem como sobre as medidas de cibersegurança adotadas por entidades críticas. A pedido das autoridades competentes ao abrigo da Diretiva (UE) XXX/XXX, as autoridades competentes ao abrigo da presente diretiva devem poder exercer as suas competências de supervisão e execução coerciva em relação a uma entidade essencial identificada como crítica. Ambas as autoridades devem cooperar e trocar informações para este fim.

(15) A proteção e conservação de um sistema de nomes de domínio (DNS) fiável, resiliente e seguro é um fator crucial para manter a integridade da Internet, sendo igualmente essencial para a continuidade e a estabilidade do seu funcionamento, das quais a sociedade e a economia digital dependem. Consequentemente, a presente diretiva deve ser aplicável a todos os prestadores de serviços de DNS ao longo da cadeia de resolução do DNS, incluindo operadores de servidores de nomes da zona raiz, servidores de nomes de domínio de topo, servidores de nomes com autoridade para nomes de domínio e servidores recursivos.

(16) Os serviços de computação em nuvem devem abranger serviços que permitam um amplo acesso remoto e a administração a pedido de um conjunto modulável e adaptável de recursos de computação partilháveis e distribuídos. Esses recursos de computação incluem redes, servidores ou outras infraestruturas, sistemas operativos, *software*, armazenamento, aplicações e serviços. Os modelos de implantação de serviços de computação em nuvem devem incluir soluções de nuvem privada, comunitária, pública e híbrida. Os serviços e os modelos de implantação supramencionados têm o mesmo significado que as condições de serviço e os modelos de implantação definidos na norma ISO/IEC 17788:2014. A possibilidade de o utilizador de serviços de computação em nuvem gerir autónoma e unilateralmente as capacidades de computação, como o tempo de acesso ao servidor ou o armazenamento em rede, sem qualquer interação humana do prestador do serviço de computação em nuvem, pode ser descrita como administração a pedido. O termo «amplo acesso remoto» é utilizado para descrever o facto de as capacidades de computação em

[17] *[Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos]*.

nuvem serem disponibilizadas através da rede e acedidas através de mecanismos que promovem a utilização de diferentes plataformas para clientes «magros» (*thin client*) ou «gordos» (*thick/fat client*) (nomeadamente telemóveis, tabletes, computadores portáteis, estações de trabalho). O termo «modulável» refere-se a recursos de computação atribuídos de forma flexível pelo prestador de serviços de computação em nuvem, independentemente da localização geográfica dos recursos, a fim de fazer face às flutuações da procura. O termo «conjunto adaptável» é utilizado para descrever os recursos de computação disponibilizados e libertados em função da procura, a fim de aumentar ou diminuir rapidamente os recursos disponíveis, consoante o volume de trabalho. O termo «partilhável» é utilizado para descrever os recursos de computação fornecidos a múltiplos utilizadores que partilham um acesso comum ao serviço, mas cujo processamento é efetuado separadamente para cada utilizador, embora o serviço seja prestado a partir do mesmo equipamento eletrónico. O termo «distribuído» é utilizado para descrever os recursos de computação localizados em diferentes computadores ou dispositivos ligados em rede, que comunicam e se coordenam entre si por via da transmissão de mensagens.

(17) Dada a emergência de tecnologias inovadoras e de novos modelos de negócio, espera-se que surjam novos modelos de serviços e de implantação da computação em nuvem no mercado em resposta à evolução das necessidades dos consumidores. Nesse contexto, os serviços de computação em nuvem poderão ser prestados sob uma forma altamente distribuída, ainda mais próxima do ponto de geração ou recolha dos dados, substituindo assim o modelo tradicional por um modelo altamente distribuído (a denominada «computação periférica»).

(18) Os serviços oferecidos por prestadores de serviços de centro de dados nem sempre serão prestados sob a forma de serviço de computação em nuvem. Consequentemente, os centros de dados nem sempre farão parte de uma infraestrutura de computação em nuvem. A fim de gerir todos os riscos que se colocam à segurança das redes e dos sistemas de informação, a presente diretiva deve abranger também os prestadores de serviços de centro de dados que não sejam serviços de computação em nuvem. Para efeitos da presente diretiva, o termo «serviço de centro de dados» deve abranger a prestação de um serviço que englobe estruturas ou grupos de estruturas dedicados ao alojamento centralizado, interligação e operação de equipamento de redes e tecnologias da informação que preste serviços de armazenamento, tratamento e transmissão de dados, juntamente com todas as instalações e infraestruturas de distribuição de energia e controlo ambiental. O termo «serviço de centro de dados» não se aplica aos centros de dados internos das empresas, detidos e geridos para os próprios fins da entidade em causa.

(19) Os prestadores de serviços postais, na aceção da Diretiva 97/67/CE do Parlamento Europeu e do Conselho[18], bem como os prestadores de serviços de correio expresso e estafeta, devem ser abrangidos pela presente diretiva se realizarem, pelo menos, uma das atividades na cadeia de entrega postal, em especial recolha, triagem ou distribuição, incluindo serviços de levantamento. Os serviços de transporte que não sejam prestados em conjunto com uma dessas atividades não devem estar abrangidos pelo âmbito dos serviços postais.

[18] Diretiva 97/67/CE do Parlamento Europeu e do Conselho, de 15 de dezembro de 1997, relativa às regras comuns para o desenvolvimento do mercado interno dos serviços postais comunitários e a melhoria da qualidade de serviço (JO L 15 de 21.1.1998, p. 14).

(20) Estas crescentes interdependências resultam de uma rede de prestação de serviços com um caráter cada vez mais transfronteiriço e interdependente, que utiliza infraestruturas essenciais em toda a União nos setores da energia, dos transportes, das infraestruturas digitais, da água potável e das águas residuais, da saúde, de certos aspetos da administração pública, bem como no setor do espaço no que se refere à prestação de certos serviços que dependem de infraestruturas terrestres detidas, geridas e operadas por Estados-Membros ou por entidades privadas, não abrangendo, portanto, as infraestruturas detidas, geridas ou operadas pela União ou em seu nome no âmbito dos seus programas espaciais. Em virtude dessas interdependências, qualquer perturbação, mesmo que inicialmente confinada a uma entidade ou a um setor, pode ter repercussões mais vastas e causar impactos negativos generalizados e duradouros na prestação de serviços em todo o mercado interno. A pandemia de COVID-19 revelou a vulnerabilidade das nossas sociedades, cada vez mais interdependentes, perante riscos com baixa probabilidade de ocorrência.

(21) Tendo em conta as diferenças nas estruturas governativas nacionais, e a fim de salvaguardar os acordos setoriais já existentes ou os organismos de supervisão e regulação da União, os Estados-Membros devem poder designar mais do que uma autoridade nacional competente para desempenhar as funções associadas à segurança das redes e dos sistemas de informação de entidades essenciais e importantes nos termos da presente diretiva. Os Estados-Membros devem poder atribuir essas funções a uma autoridade existente.

(22) A fim de facilitar a cooperação e a comunicação transfronteiriça entre as autoridades e permitir a aplicação eficaz da presente diretiva, é necessário que cada Estado-Membro designe um ponto de contacto único nacional responsável pela coordenação das questões relativas à segurança das redes e dos sistemas de informação e pela cooperação transfronteiriça a nível da União.

(23) As autoridades competentes ou as CSIRT devem receber as notificações de incidentes efetuadas pelas entidades de forma eficaz e eficiente. Os pontos de contacto únicos devem ser incumbidos do reencaminhamento das notificações de incidentes para os pontos de contacto únicos de outros Estados-Membros afetados. A fim de garantir a existência de um ponto de entrada único ao nível das autoridades de cada Estado-Membro, os pontos de contacto únicos devem ser também os destinatários de informações sobre incidentes respeitantes a entidades do setor financeiro fornecidas pelas autoridades competentes ao abrigo do Regulamento XXXX/XXXX, informações essas que deverão poder transmitir, conforme adequado, às autoridades nacionais competentes nesse domínio ou às CSIRT ao abrigo da presente diretiva.

(24) Os Estados-Membros devem estar adequadamente equipados, em termos de capacidade técnica e organizativa, para evitar, detetar e atenuar os incidentes e os riscos ligados às redes e aos sistemas de informação, e para os enfrentar. Por conseguinte, devem dispor de CSIRT, também conhecidas por equipas de resposta a emergências informáticas (CERT), que funcionem bem e que preencham os requisitos essenciais para garantir capacidades efetivas e compatíveis para fazer face aos incidentes e aos riscos e para assegurar uma cooperação eficaz a nível da União. No intuito de melhorar a relação de confiança entre as entidades e as CSIRT, nos casos em que a autoridade competente disponha de uma CSIRT, os Estados-Membros devem ponderar a separação funcional entre as funções operacionais desempenhadas pelas CSIRT, especialmente no que respeita à partilha de informações e ao apoio às entidades, e as atividades de supervisão das autoridades competentes.

(25) No que respeita a dados pessoais, as CSIRT devem poder facultar, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[19], em nome ou a pedido de uma entidade ao abrigo da presente diretiva, uma análise proativa da rede e dos sistemas de segurança utilizados para prestarem os seus serviços. Os Estados-Membros devem procurar garantir que todas as CSIRT setoriais possuam o mesmo nível de capacidades técnicas. Os Estados-Membros poderão solicitar a assistência da Agência da União Europeia para a Cibersegurança (ENISA) no desenvolvimento de CSIRT nacionais.

(26) Tendo em conta a importância da cooperação internacional em matéria de cibersegurança, as CSIRT devem poder participar em redes de cooperação internacional, em complemento da rede de CSIRT criada pela presente diretiva.

(27) Nos termos do anexo da Recomendação (UE) 2017/1548 da Comissão, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala («plano de ação»)[20], entende-se por incidente em larga escala um incidente com um impacto significativo em, pelo menos, dois Estados-Membros ou que cause perturbações tão extensas que ultrapassem a capacidade de resposta de um Estado-Membro. Consoante a sua causa e o seu impacto, os incidentes em grande escala poderão agravar-se e transformar-se em verdadeiras crises que impeçam o correto funcionamento do mercado interno. Tendo em conta o vasto alcance e, em muitos casos, o caráter transfronteiriço de tais incidentes, é importante que os Estados-Membros e as instituições, organismos e agências competentes da União cooperem a nível técnico, operacional e político para coordenarem eficazmente a resposta em toda a União.

(28) Uma vez que a exploração das vulnerabilidades das redes e dos sistemas de informação pode causar perturbações e danos consideráveis, a celeridade na identificação e correção de tais vulnerabilidades é um fator importante na redução dos riscos de cibersegurança. As entidades que desenvolvem esses sistemas devem, por conseguinte, estabelecer procedimentos adequados para fazer face a vulnerabilidades quando estas sejam detetadas. Uma vez que as vulnerabilidades são frequentemente detetadas e notificadas (divulgadas) por terceiros (entidades notificadoras), o fabricante ou fornecedor de produtos ou prestador de serviços de TIC deve adotar igualmente os procedimentos necessários para receber informações sobre vulnerabilidades fornecidas por terceiros. Nesta matéria, as normas internacionais ISO/IEC 30111 e ISO/IEC 29417 fornecem orientações sobre o tratamento de vulnerabilidades e a divulgação de vulnerabilidades, respetivamente. No que respeita à divulgação de vulnerabilidades, a coordenação entre as entidades notificadoras e os fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC assume especial importância. A divulgação coordenada de vulnerabilidades especifica um processo estruturado mediante o qual as vulnerabilidades são notificadas às organizações de uma forma que lhes permite diagnosticar e corrigir as vulnerabilidade antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público. A divulgação coordenada de vulnerabilidades deve abranger também a

---

19 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

20 Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

coordenação entre a entidade notificadora e a organização no que respeita ao momento da correção e da publicação das vulnerabilidades.

(29) Por conseguinte, os Estados-Membros devem tomar medidas para facilitar a divulgação coordenada de vulnerabilidades, definindo uma política nacional nessa matéria. Neste contexto, os Estados-Membros devem designar uma CSIRT que assuma o papel de «coordenadora», agindo como intermediária entre as entidades notificadoras e os fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC, quando necessário. As funções da CSIRT coordenadora devem incluir, em especial, a identificação e o contacto das entidades em causa, a prestação de apoio às entidades notificadoras, a negociação do calendário de divulgação de vulnerabilidades e a gestão da divulgação de vulnerabilidades que afetem várias organizações (divulgação de vulnerabilidades a várias partes). Se as vulnerabilidades afetarem vários fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC estabelecidos em mais do que um Estado-Membro, as CSIRT designadas por cada um dos Estados-Membros afetados devem cooperar no âmbito da rede de CSIRT.

(30) O acesso em tempo útil a informações fidedignas sobre vulnerabilidades que afetem produtos e serviços de TIC contribui para melhorar a gestão dos riscos de cibersegurança. Nesse contexto, as fontes de informações públicas sobre vulnerabilidades constituem um instrumento importante não só para as entidades e os seus utilizadores, mas também para as autoridades nacionais competentes e as CSIRT. Por este motivo, a ENISA deve criar um registo de vulnerabilidades no qual as entidades essenciais e importantes e os respetivos fornecedores, bem como as entidades não abrangidas pelo âmbito da presente diretiva, possam, a título voluntário, divulgar vulnerabilidades e fornecer as informações conexas que permitam aos utilizadores tomarem medidas de atenuação adequadas.

(31) Embora já existam bases de dados ou registos de vulnerabilidades semelhantes, as entidades responsáveis pelo seu alojamento e manutenção não estão estabelecidas na União. Um registo europeu de vulnerabilidades mantido pela ENISA melhoraria a transparência do processo de publicação antes de a vulnerabilidade ser oficialmente divulgada, bem como a resiliência em casos de perturbação ou interrupção da prestação de serviços semelhantes. A fim de evitar a duplicação de esforços e de assegurar, tanto quanto possível, a complementaridade, é importante que a ENISA explore a possibilidade de celebrar acordos de cooperação estruturados com registos semelhantes em jurisdições de países terceiros.

(32) O grupo de cooperação deve elaborar, de dois em dois anos, um programa de trabalho que defina as ações a empreender pelo grupo no sentido de cumprir os seus objetivos e as suas funções. O calendário do primeiro programa adotado ao abrigo da presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148, a fim de evitar potenciais perturbações das atividades do grupo.

(33) Ao elaborar documentos de orientação, o grupo de cooperação deve consistentemente: fazer um levantamento das experiências e soluções nacionais, avaliar o impacto dos resultados do trabalho do grupo de coordenação nas abordagens nacionais, discutir os desafios que se colocam à aplicação e formular recomendações específicas a adotar por via de uma melhor aplicação das regras existentes.

(34) O grupo de cooperação deve continuar a ser um fórum flexível e estar apto a reagir a alterações das prioridades e desafios políticos ou a novas prioridades e desafios políticos, tendo simultaneamente em conta a disponibilidade de recursos. Deve

organizar regularmente reuniões conjuntas com partes interessadas privadas de toda a União para discutir as atividades desenvolvidas pelo grupo e partilhar pontos de vista sobre novos desafios políticos. A fim de reforçar a cooperação a nível da União, o grupo deve equacionar a possibilidade de convidar organismos e agências da União envolvidas na política de cibersegurança, como o Centro Europeu da Cibercriminalidade (EC3), a Agência da União Europeia para a Segurança da Aviação (EASA) e a Agência da União Europeia para o Programa Espacial (EUSPA), a participarem nos seus trabalhos.

(35) As autoridades competentes e as CSIRT devem estar habilitadas a participar em programas de intercâmbio de funcionários com outros Estados-Membros, no intuito de reforçar a cooperação. As autoridades competentes devem tomar as medidas necessárias para permitir que os funcionários de outros Estados-Membros participem ativamente nas atividades da autoridade competente de acolhimento.

(36) Quando adequado, a União deve celebrar, em conformidade com o artigo 218.º do TFUE, acordos internacionais com países terceiros ou organizações internacionais que permitam e rejam a participação destes em algumas atividades do grupo de cooperação e da rede de CSIRT. Tais acordos devem assegurar uma proteção adequada dos dados.

(37) Os Estados-Membros devem contribuir para a criação do quadro de resposta da UE a crises de cibersegurança previsto na Recomendação (UE) 2017/1584 por intermédio das redes de cooperação existentes, nomeadamente a Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe), a rede de CSIRT e o grupo de cooperação. A UE-CyCLONe e a rede de CSIRT devem cooperar com base em disposições processuais que definam as modalidades dessa cooperação. O regulamento interno da UE-CyCLONe deve especificar as modalidades de funcionamento da rede, incluindo, entre outros aspetos, as funções, os modos de cooperação, as interações com outros intervenientes relevantes e os modelos de partilha de informações, bem como os meios de comunicação. No atinente à gestão de crises a nível da União, as partes responsáveis devem recorrer ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR). A Comissão deve utilizar, para este efeito, o processo de alto nível para a coordenação de crises transetoriais do sistema geral de alerta rápido (ARGUS). Se a crise implicar uma dimensão importante a nível externo ou da política comum de segurança e defesa (PCSD), deve ser ativado o mecanismo de resposta a situações de crise (CRM) do Serviço Europeu para a Ação Externa (SEAE).

(38) Para efeitos da presente diretiva, entende-se por «risco» a possibilidade de perda ou perturbação causada por um incidente de cibersegurança, a qual deve ser expressa como uma combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do referido incidente.

(39) Para efeitos da presente diretiva, entende-se por «quase incidente» um evento que poderia ter causado danos, mas que foi impedido de se materializar plenamente.

(40) As medidas de gestão de riscos devem incluir medidas para identificar os riscos de incidentes, para evitar, detetar e tratar os incidentes e para atenuar o seu impacto. A segurança das redes e dos sistemas de informação deve abranger a segurança dos dados armazenados, transmitidos e tratados.

(41) Para evitar impor encargos financeiros e administrativos desproporcionados às entidades essenciais e importantes, os requisitos estabelecidos em matéria de gestão dos riscos de cibersegurança devem ser proporcionados em relação ao risco

apresentado pelas redes e pelos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas.

(42) As entidades essenciais e importantes devem garantir a segurança das redes e dos sistemas de informação que utilizam nas suas atividades. Trata-se principalmente de redes e sistemas de informação privados geridos por pessoal interno especializado em TI ou cuja segurança tenha sido externalizada. Os requisitos em matéria de gestão dos riscos de cibersegurança e de notificação estabelecidos na presente diretiva devem aplicar-se às entidades essenciais e importantes abrangidas, independentemente de a manutenção das suas redes e sistemas de informação ser realizada a nível interno ou externalizada.

(43) Tendo em conta a frequência de incidentes em que as entidades foram vítimas de ciberataques e em que intervenientes maliciosos conseguiram pôr em causa a segurança das redes e dos sistemas de informação de uma entidade mediante a exploração de vulnerabilidades que afetam produtos e serviços de terceiros, é particularmente importante gerir os riscos de cibersegurança decorrentes da cadeia de fornecimento de uma entidade e da relação desta com os seus fornecedores. Por conseguinte, as entidades devem avaliar e ter em conta a qualidade global dos produtos e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro.

(44) Entre os prestadores de serviços, os prestadores de serviços de segurança geridos em domínios como a resposta a incidentes, os testes de penetração, as auditorias de segurança e a consultoria desempenham um papel especialmente importante em termos de apoio aos esforços desenvolvidos pelas entidades para detetar e responder a incidentes. Porém, os próprios prestadores de serviços de segurança geridos têm sido igualmente alvo de ciberataques e, em virtude da sua estreita integração nas atividades dos operadores, colocam um risco especial de cibersegurança. As entidades devem, assim, exercer uma diligência acrescida ao selecionarem um prestador de serviços de segurança geridos.

(45) As entidades devem igualmente gerir os riscos de cibersegurança emergentes da sua interação e da sua relação com outras partes interessadas no seio de um ecossistema mais vasto. Mais concretamente, as entidades devem tomar medidas adequadas para garantir que a sua cooperação com instituições académicas e de investigação respeita as suas políticas de cibersegurança e segue boas práticas no tocante ao acesso e à disseminação de informações em condições de segurança, em geral, e à proteção da propriedade intelectual, em particular. Do mesmo modo, dada a importância e o valor dos dados para as atividades das entidades, quando recorrerem a serviços de transformação de dados e de análise de dados prestados por terceiros, as entidades devem tomar todas as medidas de cibersegurança adequadas.

(46) A fim de melhorar a gestão dos principais riscos da cadeia de fornecimento e de ajudar as entidades que atuam em setores abrangidos pela presente diretiva a gerirem adequadamente riscos de cibersegurança relacionados com a cadeia de fornecimento e os fornecedores, o grupo de cooperação, com a participação das autoridades nacionais competentes e em cooperação com a Comissão e a ENISA, deve realizar avaliações setoriais coordenadas dos riscos associados às cadeias de fornecimento, tal como foi já feito para as redes 5G na sequência da Recomendação (UE) 2019/534 sobre a

cibersegurança das redes 5G[21], com o objetivo de identificar, em cada setor, os produtos, sistemas ou serviços de TIC críticos, bem como as vulnerabilidades e ameaças importantes.

(47) Dadas as características do setor em causa, as avaliações dos riscos associados às cadeias de fornecimento devem ter em conta tanto fatores técnicos como, quando pertinente, fatores não técnicos, incluindo os definidos na Recomendação (UE) 2019/534, na avaliação coordenada dos riscos de segurança das redes 5G a nível da UE, e no conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G acordado pelo grupo de cooperação. Na identificação das cadeias de fornecimento que devem estar sujeitas a uma avaliação coordenada dos riscos, importa ter em conta os seguintes critérios: i) em que medida as entidades essenciais e importantes utilizam e dependem de produtos, sistemas ou serviços de TIC críticos específicos; ii) a importância de produtos, sistemas ou serviços de TIC críticos específicos para o desempenho de funções críticas ou sensíveis, incluindo o tratamento de dados pessoais; iii) a disponibilidade de produtos, sistemas ou serviços de TIC alternativos; iv) a resiliência da cadeia global de fornecimento de produtos, sistemas ou serviços de TIC face a perturbações; v) no que respeita a produtos, sistemas ou serviços de TIC emergentes, a sua potencial importância futura para as atividades das entidades.

(48) A fim de simplificar as obrigações legais impostas aos fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público e aos prestadores de serviços de confiança, relacionadas com a segurança das respetivas redes e sistemas de informação, bem como para permitir que essas entidades e as respetivas autoridades competentes beneficiem do quadro jurídico estabelecido pela presente diretiva (incluindo a designação de CSIRT responsáveis pela gestão de riscos e pelo tratamento de incidentes, a participação de organismos e autoridades competentes no trabalho do grupo de cooperação e da rede de CSIRT), as referidas entidades devem estar abrangidas pelo âmbito de aplicação da presente diretiva. Por conseguinte, é necessário revogar as correspondentes disposições do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho[22] e da Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho[23] relacionadas com a imposição de obrigações em matéria de segurança e notificação a estes tipos de entidades. As regras em matéria de obrigações de notificação devem ser aplicáveis sem prejuízo das disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[24].

(49) Quando adequado e para evitar perturbações desnecessárias, as orientações nacionais em vigor e a legislação nacional adotada para efeitos de transposição das regras relacionadas com medidas de segurança estabelecidas no artigo 40.º, n.º 1, da Diretiva (UE) 2018/1972, bem como dos requisitos do artigo 40.º, n.º 2, da mesma diretiva respeitantes aos parâmetros utilizados para determinar a importância de um

---

21 Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, Cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).

22 Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

23 Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (JO L 321 de 17.12.2018, p. 36).

24 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

incidente, devem continuar a ser aplicadas pelas autoridades competentes encarregadas da supervisão e execução coerciva para efeitos da presente diretiva.

(50) Dada a importância crescente dos serviços de comunicações interpessoais independentes do número, é necessário assegurar que tais serviços também estejam sujeitos a requisitos de segurança adequados, tendo em conta a sua natureza específica e importância económica. Assim, os prestadores de tais serviços devem igualmente garantir um nível de segurança das redes e dos sistemas de informação adequado aos riscos que representam. Dado que, por norma, os prestadores de serviços de comunicações interpessoais independentes do número não exercem um controlo efetivo sobre a transmissão de sinais através das redes, o nível de risco desses serviços poderá considerar-se, sob determinados aspetos, inferior ao dos serviços de comunicações eletrónicas tradicionais. O mesmo é válido para os serviços de comunicações interpessoais que utilizam números e que não exercem um controlo efetivo sobre a transmissão de sinais.

(51) O mercado interno depende, mais do que nunca, do funcionamento da Internet. Os serviços de praticamente todas as entidades essenciais e importantes estão dependentes de serviços prestados através da Internet. Para evitar problemas na prestação dos serviços assegurados por entidades essenciais e importantes, é necessário que as redes públicas de comunicações eletrónicas, por exemplo as estruturas de base da Internet ou os cabos submarinos de comunicações, adotem medidas de cibersegurança adequadas e notifiquem incidentes relacionados com as mesmas.

(52) Quando adequado, as entidades devem informar os destinatários dos seus serviços sobre ameaças específicas e graves e sobre as medidas que podem tomar para minimizar o risco delas resultantes a que estão expostos. A exigência de informar os referidos destinatários de tais ameaças não deve isentar as entidades da obrigação de, a expensas suas, adotarem medidas adequadas e imediatas para prevenir ou remediar quaisquer ciberameaças e restabelecer o nível normal de segurança do serviço. A prestação dessas informações aos destinatários sobre ameaças à segurança deve ser gratuita.

(53) Em especial, os fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público devem informar os destinatários dos serviços sobre ameaças específicas e graves em matéria de cibersegurança e sobre as medidas que podem tomar para proteger a segurança das suas comunicações, por exemplo, recorrendo a tipos específicos de *software* ou tecnologias de cifragem.

(54) Para salvaguardar a segurança das redes e serviços de comunicações eletrónicas, a utilização de cifragem, especialmente da cifragem de ponta a ponta, deve ser promovida e, se necessário, deve ser obrigatória para os fornecedores das referidas redes e serviços, em conformidade com os princípios da segurança e da privacidade por defeito e desde a conceção para efeitos do artigo 18.º. A utilização da cifragem de ponta a ponta deve ser conciliada com os poderes que os Estados-Membros detêm para assegurar a proteção dos seus interesses essenciais de segurança e da segurança pública e para permitir a investigação, a deteção e a repressão de infrações penais em conformidade com o direito da União. As soluções de acesso lícito a informações em comunicações cifradas de ponta a ponta devem manter a eficácia da cifragem em termos de proteção da privacidade e da segurança das comunicações, proporcionando simultaneamente uma resposta eficaz à criminalidade.

(55) A presente diretiva define uma abordagem em duas etapas à notificação de incidentes, a fim de estabelecer o equilíbrio adequado entre, por um lado, uma notificação célere que ajude a minimizar a potencial propagação de incidentes e permita às entidades procurar apoio e, por outro lado, uma notificação exaustiva que retire ensinamentos valiosos de incidentes individuais e melhore gradualmente a resiliência de empresas individuais e setores inteiros face às ciberameaças. Quando tenham tido conhecimento de um incidente, as entidades devem ser obrigadas a efetuar uma notificação inicial no prazo de 24 horas, seguida pela apresentação de um relatório final, o mais tardar, um mês depois. A notificação inicial deve conter apenas as informações estritamente necessárias para dar conhecimento do incidente às autoridades competentes e para permitir que a entidade procure assistência, caso tal seja necessário. Se for o caso, a referida notificação deve indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso. Os Estados-Membros devem garantir que a obrigação de apresentar esta notificação inicial não desvia os recursos da entidade notificadora afetos a atividades relacionadas com o tratamento de incidentes, às quais deve ser atribuída prioridade. Para evitar que as obrigações de notificação de incidentes desviem recursos afetos à resposta a incidentes ou possam prejudicar, de qualquer outra forma, os esforços desenvolvidos pelas entidades nessa matéria, os Estados-Membros devem igualmente estabelecer que, em casos devidamente justificados e com a concordância das autoridades competentes ou da CSIRT, a entidade em causa poderá não cumprir o prazo de 24 horas para a notificação inicial ou o prazo de um mês para o relatório final.

(56) As entidades essenciais e importantes encontram-se frequentemente numa situação em que um determinado incidente, por força das suas características, tem de ser comunicado a várias autoridades em cumprimento de obrigações de notificação estabelecidas em diferentes instrumentos jurídicos. Essas situações criam encargos adicionais, podendo igualmente gerar dúvidas quanto ao formato e aos procedimentos aplicáveis a tais notificações. Por este motivo, e com o objetivo de simplificar a notificação de incidentes de segurança, os Estados-Membros devem estabelecer *um ponto de entrada único* para todas as notificações exigidas pela presente diretiva e também por outros instrumentos jurídicos da União, como o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. A ENISA, em cooperação com o grupo de cooperação, deve criar modelos comuns de notificação por intermédio de orientações destinadas a simplificar e racionalizar a comunicação de informações exigidas pelo direito da União e a reduzir os encargos para as empresas.

(57) Os Estados-Membros devem incentivar as entidades essenciais e importantes, com base nas regras de processo penal aplicáveis e em conformidade com o direito da União, a notificar às autoridades policiais competentes os incidentes que se suspeite estarem relacionados com atividades criminosas graves nos termos do direito da União ou do direito nacional. Em determinados casos, e sem prejuízo das regras relativas à proteção de dados pessoais aplicáveis à Europol, é desejável que o Centro Europeu da Cibercriminalidade (EC3) e a ENISA facilitem a coordenação entre as autoridades competentes e as autoridades policiais dos diferentes Estados-Membros.

(58) Os dados pessoais ficam amiúde expostos em consequência de incidentes. Neste contexto, as entidades competentes devem cooperar e trocar informações sobre todas as questões pertinentes com as autoridades de proteção de dados e as autoridades de fiscalização nos termos da Diretiva 2002/58/CE.

(59) A manutenção de bases de dados fidedignas e completas dos nomes de domínio e dados de registo (os chamados «dados WHOIS») e a concessão de acesso lícito a tais

dados é essencial para garantir a segurança, estabilidade e resiliência do DNS, o que, por sua vez, contribui para um elevado nível comum de cibersegurança na União. Quando as operações de tratamento abrangerem dados pessoais, esse tratamento deve cumprir a legislação da União em matéria de proteção de dados.

(60) A disponibilização e a concessão atempada do acesso a estes dados às autoridades públicas, incluindo as autoridades competentes para a prevenção, investigação ou repressão de infrações penais ao abrigo do direito da União ou do direito nacional, às CERT, às CSIRT e, no que respeita aos dados dos seus clientes, aos fornecedores de redes e serviços de comunicações eletrónicas e aos fornecedores de tecnologias e serviços de cibersegurança que atuam em nome desses clientes, são fatores essenciais para prevenir e combater abusos do sistema de nomes de domínio, em especial para evitar, detetar e responder a incidentes de cibersegurança. Tal acesso deve respeitar a legislação da União em matéria de proteção de dados, na medida em que diga respeito a dados pessoais.

(61) A fim de assegurar a disponibilidade de dados exatos e completos relativos ao registo de nomes de domínio, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos (os chamados agentes de registo) devem recolher dados relativos ao registo de nomes de domínio e garantir a integridade e disponibilidade desses dados. Em especial, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem estabelecer políticas e procedimentos para recolher e manter dados de registo exatos e completos, bem como para evitar e corrigir dados de registo incorretos, em conformidade com as regras da União em matéria de proteção de dados.

(62) Os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem disponibilizar ao público dados relativos ao registo de nomes de domínio que não estejam abrangidos pelo âmbito das regras da União em matéria de proteção de dados, como os dados respeitantes a pessoas coletivas[25]. Os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem igualmente permitir o acesso lícito a dados específicos de registo de nomes de domínio respeitantes a pessoas singulares aos requerentes legítimos de acesso, em conformidade com a legislação da União em matéria de proteção de dados. Os Estados-Membros devem assegurar que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos estejam obrigados a responder, sem demora injustificada, a pedidos de divulgação de dados relativos ao registo de nomes de domínio apresentados por requerentes legítimos de acesso. Estes registos e entidades devem estabelecer políticas e procedimentos com vista à publicação e divulgação de dados de registo, incluindo acordos de nível de serviço, a fim de responder a pedidos de acesso apresentados por requerentes legítimos de acesso. O procedimento de acesso pode também contemplar a utilização de uma interface, de um portal ou de outra ferramenta técnica para disponibilizar um sistema eficiente de pedido e acesso a dados de registo. A fim de promover práticas harmonizadas em todo o mercado interno, a Comissão pode adotar orientações sobre tais procedimentos, sem prejuízo das competências do Comité Europeu para a Proteção de Dados.

[25] Considerando 14 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, nos termos do qual «[o] presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva».

(63) Todas as entidades essenciais e importantes abrangidas pela presente diretiva devem estar sob a jurisdição do Estado-Membro onde prestam os seus serviços. Se uma entidade prestar serviços em mais do que um Estado-Membro, deve estar sob a jurisdição autónoma e concorrente de cada um desses Estados-Membros. As autoridades competentes desses Estados-Membros devem cooperar, prestar assistência mútua e, se for o caso, realizar ações de supervisão conjuntas.

(64) Para ter em conta a natureza transfronteiriça dos serviços e operações dos prestadores de serviços de DNS, dos registos de nomes de domínio de topo, dos fornecedores de redes de distribuição de conteúdos, dos prestadores de serviços de computação em nuvem, dos prestadores de serviços de centro de dados e dos prestadores de serviços digitais, estas entidades devem estar sob a jurisdição de um único Estado-Membro. A competência deve ser atribuída ao Estado-Membro onde a respetiva entidade tem o seu estabelecimento principal na União. O critério do estabelecimento para efeitos da presente diretiva pressupõe o exercício efetivo de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto. O preenchimento deste critério não deve estar associado à presença física das redes e sistemas de informação num determinado local; a presença e utilização desses sistemas não constitui, por si só, um estabelecimento principal e, consequentemente, não é um critério decisivo para determinar o estabelecimento principal. O estabelecimento principal deve ser o local onde as decisões relacionadas com as medidas de gestão dos riscos de cibersegurança são tomadas na União. Em regra, corresponderá ao local onde se situa a administração central das empresas na União. Se as referidas decisões não forem tomadas na União, deve considerar-se que o estabelecimento principal se localiza no Estado-Membro onde a entidade possui o estabelecimento com o maior número de trabalhadores na União. Se os serviços forem prestados por um grupo de empresas, deve considerar-se que o seu estabelecimento principal é o estabelecimento principal da empresa que exerce o controlo.

(65) Nos casos em que um prestador de serviços de DNS, um registo de nomes de domínio de topo, um fornecedor de redes de distribuição de conteúdos, um prestador de serviços de computação em nuvem, um prestador de serviços de centro de dados ou um prestador de serviços digitais não estabelecido na União ofereça serviços na União, deve designar um representante. A fim de determinar se tal entidade oferece serviços na União, há que apurar se é evidente a sua intenção de oferecer serviços a pessoas em um ou vários Estados-Membros. O mero facto de estar acessível, na União, um sítio Web da entidade ou de um intermediário ou um endereço eletrónico ou outro tipo de contactos ou de ser utilizada uma língua de uso corrente no país terceiro em que a entidade se encontra estabelecida não é, enquanto tal, suficiente para determinar essa intenção. Contudo, fatores como a utilização de uma língua ou de uma moeda de uso corrente em um ou vários Estados-Membros, com a possibilidade de encomendar serviços nessa outra língua, ou a referência a clientes ou utilizadores na União podem revelar que a entidade tenciona oferecer serviços na União. O representante deve atuar por conta da entidade e deve poder ser contactado pelas autoridades competentes ou pelas CSIRT. O representante deve ser explicitamente designado, por mandato escrito da entidade, para atuar por conta desta última relativamente às obrigações que lhe incumbem por força da presente diretiva, incluindo a notificação de incidentes.

(66) Se, ao abrigo das disposições da presente diretiva, forem trocadas, comunicadas ou de outro modo partilhadas informações consideradas classificadas nos termos do direito

nacional ou da União, devem ser aplicadas as correspondentes regras específicas sobre o tratamento de informações classificadas.

(67) Dado que as ciberameaças têm vindo a tornar-se mais complexas e sofisticadas, a eficácia das medidas de deteção e prevenção depende, em grande medida, da partilha regular de informações sobre ameaças e vulnerabilidades entre entidades. A partilha de informações contribui para uma maior sensibilização para as ciberameaças, o que, por sua vez, reforça a capacidade das entidades para impedirem que as ameaças se tornem em verdadeiros incidentes e permite que as entidades contenham melhor os efeitos dos incidentes e recuperem de modo mais eficiente. Na ausência de orientações a nível da União, diversos fatores parecem ter impedido a referida partilha de informações, especialmente as dúvidas quanto à compatibilidade com as regras em matéria de concorrência e responsabilidade.

(68) Importa incentivar as entidades a tirarem partido, coletivamente, dos seus conhecimentos e experiências práticas individuais a nível estratégico, tático e operacional, com vista a reforçarem as suas capacidades para avaliarem, monitorizarem, se defenderem e darem resposta, de forma adequada, às ciberameaças. Consequentemente, é necessário viabilizar a criação, a nível da União, de mecanismos de partilha de informações a título voluntário. Para tal, os Estados-Membros devem apoiar ativamente e incentivar também entidades pertinentes não abrangidas pelo âmbito da presente diretiva a participarem em tais mecanismos de partilha de informações. Esses mecanismos devem respeitar plenamente as regras da União em matéria de concorrência e de proteção de dados.

(69) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, por entidades, autoridades públicas, CERT, CSIRT e fornecedores de tecnologias e serviços de segurança deve ser considerado um interesse legítimo do responsável pelo tratamento de dados em causa, tal como referido no Regulamento (UE) 2016/679. Tal deve incluir medidas relacionadas com a prevenção, deteção, análise e resposta a incidentes, medidas de sensibilização relativas a ciberameaças específicas, intercâmbio de informações no contexto da correção e da divulgação coordenada de vulnerabilidades, bem como o intercâmbio voluntário de informações sobre esses incidentes, ciberameaças e vulnerabilidades, indicadores de exposição a riscos, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração. As referidas medidas poderão implicar o tratamento dos seguintes tipos de dados pessoais: endereços IP, localizadores uniformes de recursos (URL), nomes de domínio e endereços de correio eletrónico.

(70) A fim de reforçar as ações e os poderes de supervisão que ajudam a assegurar um cumprimento efetivo, a presente diretiva deve estabelecer uma lista mínima de meios e ações de supervisão por meio dos quais as autoridades competentes poderão supervisionar entidades essenciais e importantes. Adicionalmente, a presente diretiva deve distinguir entre o regime de supervisão aplicável a entidades essenciais e a entidades importantes, com vista a garantir um equilíbrio justo das obrigações tanto para as entidades como para as autoridades competentes. Assim, as entidades essenciais devem ficar sujeitas a um regime de supervisão completo (*ex ante* e *ex post*), ao passo que as entidades importantes devem ficar sujeitas a um regime de supervisão simplificado, aplicável apenas *ex post*. Tal significa que as entidades importantes não são obrigadas a documentar sistematicamente o cumprimento dos requisitos em matéria de gestão dos riscos de cibersegurança e que as autoridades

competentes devem adotar uma abordagem *ex post* reativa à supervisão, pelo que não estão sujeitas a uma obrigação geral de supervisionar essas entidades.

(71) Para que a execução coerciva seja eficaz, há que estabelecer uma lista mínima de sanções administrativas aplicáveis em caso de incumprimento das obrigações de gestão dos riscos de cibersegurança e de notificação previstas na presente diretiva, definindo um quadro claro e consistente para tais sanções em toda a União. Importa ter em devida conta a natureza, a gravidade e a duração da infração, os danos efetivamente causados ou as perdas efetivamente sofridas, ou potenciais danos ou perdas que poderiam ter sido desencadeados, o caráter doloso ou negligente da infração, as medidas tomadas para prevenir ou atenuar os danos e/ou perdas sofridas, o grau de responsabilidade ou quaisquer infrações anteriores pertinentes, o grau de cooperação com a autoridade competente e qualquer outra circunstância agravante ou atenuante. A imposição de sanções, incluindo coimas, deve estar sujeita a garantias processuais adequadas em conformidade com os princípios gerais do direito da União e da Carta dos Direitos Fundamentais da União Europeia, incluindo o princípio da tutela jurisdicional efetiva e o direito a um processo equitativo.

(72) A fim de assegurar a execução coerciva das obrigações estabelecidas na presente diretiva, cada autoridade competente deve ter o poder de impor ou de solicitar a imposição de coimas.

(73) Sempre que forem impostas coimas a empresas, estas devem ser entendidas como empresas nos termos dos artigos 101.º e 102.º do TFUE para esse efeito. Sempre que forem impostas coimas a pessoas que não sejam empresas, a autoridade de supervisão deve ter em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em causa, no momento de estabelecer o montante adequado da coima. Deve caber aos Estados-Membros determinar se as autoridades públicas devem estar sujeitas a coimas, e em que medida. A imposição de uma coima não afeta o exercício de outros poderes pelas autoridades competentes nem a aplicação de outras sanções estabelecidas nas regras nacionais que transpõem a presente diretiva.

(74) Os Estados-Membros devem poder definir as normas relativas às sanções penais aplicáveis por infrações às regras nacionais que transpõem a presente diretiva. Contudo, a imposição de sanções penais por infrações às referidas regras nacionais e de sanções administrativas conexas não pode configurar uma violação do princípio *ne bis in idem* (não ser julgado duas vezes pelo mesmo facto), tal como interpretado pelo Tribunal de Justiça.

(75) Sempre que a presente diretiva não harmonize sanções administrativas, ou se necessário noutros casos (por exemplo, incumprimento grave das obrigações estabelecidas na presente diretiva), os Estados-Membros devem criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deve ser determinada pelo direito do Estado-Membro.

(76) Com vista a reforçar a eficácia e o caráter dissuasivo das sanções aplicáveis por incumprimento das obrigações estabelecidas nos termos da presente diretiva, as autoridades competentes devem estar habilitadas a aplicar sanções que consistam na suspensão de uma certificação ou autorização para a totalidade ou parte dos serviços prestados por uma entidade essencial e na interdição temporária do exercício de funções de administração por uma pessoa singular. Dada a sua severidade e o seu impacto nas atividades das entidades e, em última análise, nos seus clientes, as referidas sanções devem ser proporcionadas à gravidade da infração e ter em conta as circunstâncias concretas de cada caso, incluindo o caráter doloso ou negligente da

infração e as medidas tomadas para prevenir ou atenuar os danos e/ou perdas sofridas. Essas sanções só devem ser aplicadas em último recurso, ou seja, apenas depois de esgotadas todas as outras medidas coercivas pertinentes previstas na presente diretiva, e apenas até que as entidades a elas sujeitas tenham tomado as medidas necessárias para corrigir as deficiências ou satisfazer os requisitos da autoridade competente que estiveram na origem da aplicação das sanções. A imposição de tais sanções deve estar sujeita a garantias processuais adequadas em conformidade com os princípios gerais do direito da União e da Carta dos Direitos Fundamentais da União Europeia, incluindo a tutela jurisdicional efetiva, o processo equitativo, a presunção de inocência e o direito de defesa.

(77) A presente diretiva deve definir regras em matéria de cooperação entre as autoridades competentes e as autoridades de controlo, em conformidade com o Regulamento (UE) 2016/679, com vista ao tratamento de infrações relacionadas com dados pessoais.

(78) A presente diretiva deve procurar assegurar um elevado nível de responsabilidade pelas medidas de gestão dos riscos de cibersegurança e pelas obrigações de notificação ao nível das organizações. Por estes motivos, os órgãos de direção das entidades abrangidas pelo âmbito da presente diretiva devem aprovar essas medidas e fiscalizar a sua aplicação.

(79) É necessário instituir um mecanismo de análise pelos pares, no âmbito do qual peritos designados pelos Estados-Membros possam avaliar a execução das políticas de cibersegurança, bem como o nível das capacidades e de recursos disponíveis dos Estados-Membros.

(80) A fim de ter em conta novas ciberameaças, avanços tecnológicos ou especificidades setoriais, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão no que diz respeito aos elementos relativos às medidas de gestão dos riscos exigidas pela presente diretiva. A Comissão deve ficar igualmente habilitada a adotar atos delegados que especifiquem as categorias de entidades essenciais obrigadas a obter um certificado e os sistemas europeus de certificação da cibersegurança a que devem recorrer para o efeito. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[26]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(81) A fim de garantir condições uniformes para a aplicação das disposições pertinentes da presente diretiva relativas às disposições processuais necessárias ao funcionamento do grupo de cooperação, aos elementos técnicos relacionados com as medidas de gestão dos riscos ou ao tipo de informação, ao formato e ao procedimento de notificação de incidentes, é necessário atribuir competências de execução à Comissão. Essas

[26] JO L 123 de 12.5.2016, p. 1.

competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[27].

(82) A Comissão deve avaliar regularmente a presente diretiva, em consulta com todas as partes interessadas, nomeadamente para decidir da eventual necessidade de a alterar à luz da evolução das condições sociais, políticas, tecnológicas ou do mercado.

(83) Atendendo a que o objetivo da presente diretiva, a saber, atingir um elevado nível comum de cibersegurança na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação considerada, ser mais bem alcançado a nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para alcançar esse objetivo.

(84) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, em especial o direito ao respeito da vida privada e das comunicações, a proteção dos dados pessoais, a liberdade de empresa, o direito de propriedade, o direito à ação perante um tribunal e o direito a ser ouvido. A presente diretiva deve ser aplicada de acordo com esses direitos e princípios,

ADOTARAM A PRESENTE DIRETIVA:

## CAPÍTULO I

*Disposições gerais*

*Artigo 1.º*

***Objeto***

1. A presente diretiva estabelece medidas destinadas a assegurar um elevado nível comum de cibersegurança na União.

2. Para o efeito, a presente diretiva:

   a) Estabelece a obrigação de os Estados-Membros adotarem estratégias nacionais de cibersegurança e de designarem autoridades nacionais competentes, pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (CSIRT);

   b) Impõe obrigações de gestão dos riscos de cibersegurança e de notificação às entidades qualificadas como entidades essenciais no anexo I e como entidades importantes no anexo II;

   c) Impõe obrigações em matéria de partilha de informações sobre cibersegurança.

[27] Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

*Artigo 2.º*

***Âmbito***

1. A presente diretiva aplica-se às entidades públicas e privadas qualificadas como entidades essenciais no anexo I e como entidades importantes no anexo II. Não se aplica às entidades consideradas micro e pequenas empresas na aceção da Recomendação 2003/361/CE da Comissão[28].

2. No entanto, a presente diretiva também se aplica às entidades referidas nos anexos I e II, independentemente da sua dimensão, nos casos em que:

   a) Os serviços são prestados por uma das seguintes entidades:

      i) fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público referidos no anexo I, ponto 8,

      ii) prestadores de serviços de confiança referidos no anexo I, ponto 8,

      iii) registos de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio (DNS) referidos no anexo I, ponto 8;

   b) A entidade é uma entidade da administração pública, na aceção do artigo 4.º, ponto 23;

   c) A entidade é o único prestador de um serviço num Estado-Membro;

   d) Uma potencial perturbação do serviço prestado pela entidade possa afetar a segurança pública, a proteção pública ou a saúde pública;

   e) Uma potencial perturbação do serviço prestado pela entidade possa gerar riscos sistémicos, especialmente para os setores onde tal perturbação possa ter um impacto transfronteiriço;

   f) A entidade é crítica devido à sua importância específica, a nível regional ou nacional, para o setor ou o tipo de serviço em causa, ou para outros setores interdependentes no Estado-Membro;

   g) A entidade tenha sido identificada como entidade crítica nos termos da Diretiva (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[29] [Diretiva Resiliência das Entidades Críticas], ou como uma entidade equivalente a uma entidade crítica nos termos do artigo 7.º da referida diretiva.

   Os Estados-Membros devem elaborar uma lista das entidades identificadas nos termos das alíneas b) a f) e apresentá-la à Comissão até [seis meses após o prazo de transposição]. Os Estados-Membros devem rever a lista regularmente, pelo menos de dois em dois anos, e atualizá-la quando necessário.

---

[28] Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

[29] *[Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos]*.

3. A presente diretiva não prejudica as competências dos Estados-Membros no domínio da manutenção da segurança pública, da defesa e da segurança nacional, em conformidade com o direito da União.

4. A presente diretiva é aplicável sem prejuízo da Diretiva 2008/114/CE do Conselho[30] e das Diretivas 2011/93/UE[31] e 2013/40/UE[32] do Parlamento Europeu e do Conselho.

5. Sem prejuízo do artigo 346.º do TFUE, as informações classificadas como confidenciais nos termos de regras da União e de regras nacionais, tais como regras em matéria de sigilo comercial, só podem ser trocadas com a Comissão e com outras autoridades competentes nos casos em que esse intercâmbio seja necessário para efeitos de aplicação da presente diretiva. As informações trocadas devem limitar-se ao que for pertinente e proporcionado em relação ao objetivo desse intercâmbio. O intercâmbio de informações deve preservar a confidencialidade dessas informações e salvaguardar a segurança e os interesses comerciais das entidades essenciais ou importantes.

6. Nos casos em que disposições de atos setoriais de direito da União exijam que entidades essenciais ou importantes adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes ou ciberameaças significativas, e se tais exigências forem, na prática, pelo menos equivalentes às obrigações estabelecidas na presente diretiva, as correspondentes disposições desta última, incluindo a disposição em matéria de supervisão e execução coerciva estabelecida no capítulo VI, não se aplicam.

*Artigo 3.º*

***Harmonização mínima***

Sem prejuízo de outras obrigações que lhes incubem por força do direito da União, os Estados-Membros podem, em conformidade com a presente diretiva, adotar ou manter disposições que garantam um elevado nível de cibersegurança.

*Artigo 4.º*

***Definições***

Para efeitos da presente diretiva, entende-se por:

1) «Rede e sistema de informação»:

   a) Uma rede de comunicações eletrónicas na aceção do artigo 2.º, ponto 1, da Diretiva (UE) 2018/1972;

---

30 Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

31 Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO L 335 de 17.12.2011, p. 1).

32 Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8).

b) Um dispositivo ou um grupo de dispositivos interligados ou associados, dos quais um ou vários efetuam o tratamento automático de dados digitais com base num programa;

c) Os dados digitais armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas a) e b) tendo em vista a sua exploração, utilização, proteção e manutenção;

2) «Segurança das redes e dos sistemas de informação»: a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que ponham em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis por intermédio destes;

3) «Cibersegurança»: cibersegurança na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[33];

4) «Estratégia nacional de cibersegurança»: um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos em matéria de segurança das redes e dos sistemas de informação a nível nacional;

5) «Incidente»: qualquer evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços conexos oferecidos por redes e sistemas de informação ou acessíveis por intermédio destes;

6) «Tratamento de incidentes»: todas as ações e procedimentos que visam a deteção, a análise e a contenção de um incidente, bem como a resposta a um incidente;

7) «Ciberameaça»: uma ciberameaça na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/881;

8) «Vulnerabilidade»: um ponto fraco, uma suscetibilidade ou uma falha de um ativo, sistema, processo ou controlo passível de ser explorada por uma ciberameaça;

9) «Representante»: uma pessoa singular ou coletiva estabelecida na União, expressamente designada para atuar por conta de: i) um prestador de serviços de DNS, um registo de nomes de domínio de topo, um prestador de serviços de computação em nuvem, um prestador de serviços de centro de dados, um fornecedor de redes de distribuição de conteúdos, referidos no anexo I, ponto 8, ou ii) entidades referidas no anexo II, ponto 6, que não se encontrem estabelecidas na União, que possa ser contactada por uma autoridade nacional competente ou por uma CSIRT, em vez da entidade representada, quanto às obrigações que incumbem a esta última por força da presente diretiva;

10) «Norma»: uma norma na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho[34];

---

[33] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

[34] Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e

11) «Especificação técnica»: uma especificação técnica na aceção do artigo 2.º, ponto 4, do Regulamento (UE) n.º 1025/2012;

12) «Ponto de troca de tráfego (IXP)»: uma estrutura de rede que permite a interligação de mais de duas redes independentes (sistemas autónomos), sobretudo a fim de facilitar a troca de tráfego na Internet; um ponto de troca de tráfego só interliga sistemas autónomos; um ponto de troca de tráfego não implica que o tráfego na Internet entre um par de sistemas autónomos participantes passe através de um terceiro sistema autónomo, não altera esse tráfego nem interfere nele de qualquer outra forma;

13) «Sistema de nomes de domínio (DNS)»: um sistema de nomes distribuídos hierarquicamente que permite aos utilizadores finais aceder a serviços e recursos na Internet;

14) «Prestador de serviços de DNS»: uma entidade que presta serviços de resolução recursiva ou autoritativa de nomes de domínio a utilizadores finais da Internet e a outros prestadores de serviços de DNS;

15) «Registo de nomes de domínio de topo»: uma entidade a quem foi delegado um domínio de topo específico e que é responsável pela sua administração, incluindo o registo de nomes de domínio sob o domínio de topo e a operação técnica desse domínio de topo, incluindo a operação dos seus servidores de nomes, a manutenção das suas bases de dados e a distribuição de ficheiros da zona de domínios de topo pelos servidores de nomes;

16) «Serviço digital»: um serviço na aceção do artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho[35];

17) «Mercado em linha»: um serviço digital na aceção do artigo 2.º, alínea n), da Diretiva 2005/29/CE do Parlamento Europeu e do Conselho[36];

18) «Motor de pesquisa em linha»: um serviço digital na aceção do artigo 2.º, ponto 5, do Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho[37];

19) «Serviço de computação em nuvem»: um serviço digital que permite a administração a pedido e um amplo acesso remoto a um conjunto modulável e adaptável de recursos de computação partilháveis e distribuídos;

20) «Serviço de centro de dados»: um serviço que engloba estruturas ou grupos de estruturas dedicados ao alojamento, à interligação e à operação centralizadas de equipamento de redes e tecnologias da informação que preste serviços de armazenamento, tratamento e transmissão de dados, juntamente com todas as instalações e infraestruturas de distribuição de energia e controlo ambiental;

---

2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

35 Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

36 Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.º 2006/2004 («Diretiva relativa às práticas comerciais desleais») (JO L 149 de 11.6.2005, p. 22).

37 Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha (JO L 186 de 11.7.2019, p. 57).

21) «Rede de distribuição de conteúdos»: uma rede de servidores distribuídos geograficamente para o efeito de assegurar uma elevada disponibilidade, acessibilidade ou rápida distribuição de serviços e conteúdos digitais a utilizadores da Internet por conta de fornecedores de conteúdos e serviços;

22) «Plataforma de serviços de redes sociais»: uma plataforma que permite que utilizadores finais se conetem, partilhem, descubram e comuniquem entre si em vários dispositivos, especialmente por intermédio de conversas, publicações, vídeos e recomendações;

23) «Entidade da administração pública»: uma entidade num Estado-Membro que cumpra os seguintes critérios:

a) Foi criada para satisfazer necessidades de interesse geral e não tem carácter industrial ou comercial;

b) É dotada de personalidade jurídica;

c) É financiada maioritariamente pelo Estado, por autoridades regionais ou por outros organismos de direito público; ou a sua gestão está sujeita a fiscalização por parte dessas autoridades ou desses organismos; ou mais de metade dos membros dos seus órgãos de administração, direção ou fiscalização são designados pelo Estado, por autoridades regionais ou por outros organismos de direito público;

d) Tem competência para tomar decisões de natureza administrativa ou regulamentar que afetem os direitos de pessoas singulares ou coletivas no contexto da circulação transfronteiriça de pessoas, mercadorias, serviços ou capitais.

Estão excluídas as entidades da administração pública que exerçam atividades nos domínios da segurança pública, dos serviços policiais, da defesa ou da segurança nacional;

24) «Entidade»: uma pessoa singular ou coletiva criada e reconhecida como tal pelo direito nacional do seu local de estabelecimento, que pode, atuando em seu próprio nome, exercer direitos e estar sujeita a obrigações;

25) «Entidade essencial»: uma entidade de um tipo qualificado como entidade essencial no anexo I;

26) «Entidade importante»: uma entidade de um tipo qualificado como entidade importante no anexo II.

## CAPÍTULO II

Quadros regulamentares coordenados em matéria de cibersegurança

### *Artigo 5.º*
### *Estratégia nacional de cibersegurança*

1. Os Estados-Membros devem adotar uma estratégia nacional de cibersegurança que defina objetivos estratégicos e medidas políticas e regulamentares adequadas, com

vista a alcançar e a manter um elevado nível de cibersegurança. A estratégia nacional de cibersegurança deve incluir, em especial, o seguinte:

a) A definição dos objetivos e prioridades da estratégia de cibersegurança do Estado-Membro;

b) Um quadro de governação para cumprir esses objetivos e prioridades, incluindo as políticas referidas no n.º 2 e as funções e responsabilidades das entidades e organismos públicos, bem como de outros intervenientes pertinentes;

c) Uma avaliação para identificar ativos importantes e riscos de cibersegurança nesse Estado-Membro;

d) A identificação das medidas de preparação, de resposta e de recuperação em caso de incidentes, incluindo a cooperação entre os setores público e privado;

e) Uma lista das diversas autoridades e intervenientes envolvidos na execução da estratégia nacional de cibersegurança;

f) Um quadro político para o reforço da cooperação entre as autoridades competentes ao abrigo da presente diretiva e da Diretiva (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[38] [Diretiva Resiliência das Entidade Críticas] para efeitos de partilha de informações sobre incidentes e ciberameaças e do exercício de funções de supervisão.

2. No âmbito da estratégia nacional de cibersegurança, os Estados-Membros devem adotar, em especial, as seguintes políticas:

a) Uma política sobre a cibersegurança na cadeia de fornecimento de produtos e serviços de TIC utilizados por entidades essenciais e importantes na prestação dos seus serviços;

b) Orientação relativas à inclusão e à especificação de requisitos em matéria de cibersegurança aplicáveis a produtos e serviços de TIC nos procedimentos de contratação pública;

c) Uma política destinada a promover e facilitar a divulgação coordenada de vulnerabilidades na aceção do artigo 6.º;

d) Uma política relacionada com a manutenção da disponibilidade geral e da integridade do núcleo público da Internet aberta;

e) Uma política de promoção e desenvolvimento de competências no domínio da cibersegurança, de sensibilização e de iniciativas de investigação e desenvolvimento;

f) Uma política de apoio às instituições académicas e de investigação no desenvolvimento de ferramentas de cibersegurança e de infraestruturas de redes seguras;

g) Uma política, procedimentos e ferramentas adequadas de partilha de informações para apoiar a partilha voluntária de informações sobre cibersegurança entre as empresas, em conformidade com o direito da União;

[38] *[Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos]*.

h) Uma política para responder às necessidades específicas das PME, especialmente das que estão excluídas do âmbito da presente diretiva, no que respeita a orientações e apoio para melhorarem a sua resiliência a ciberameaças.

3. Os Estados-Membros devem notificar as suas estratégias nacionais de cibersegurança à Comissão no prazo de três meses a contar da sua adoção. Os Estados-Membros podem excluir informações específicas da notificação, na medida estritamente necessária para salvaguardar a segurança nacional.

4. Os Estados-Membros devem avaliar as suas estratégias nacionais de cibersegurança pelo menos de quatro em quatro anos com base em indicadores-chave de desempenho e, quando necessário, devem alterá-las. A pedido dos Estados-Membros, a Agência da União Europeia para a Cibersegurança (ENISA) deve ajudá-los a formular uma estratégia nacional e indicadores-chave de desempenho para a avaliação dessa estratégia.

*Artigo 6.º*

***Divulgação coordenada de vulnerabilidades e registo europeu de vulnerabilidades***

1. Cada Estado-Membro deve designar uma das suas CSIRT a que se refere o artigo 9.º como coordenadora para efeitos da divulgação coordenada de vulnerabilidades. A CSIRT designada deve desempenhar o papel de intermediário de confiança, facilitando, quando necessário, a interação entre a entidade notificadora e o fabricante ou fornecedor de produtos ou prestador de serviços de TIC. Nos casos em que a vulnerabilidade notificada diga respeito a vários fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC na União, a CSIRT designada por cada Estado-Membro em causa deve cooperar com a rede de CSIRT.

2. A ENISA deve criar e manter um registo europeu de vulnerabilidades. Para tal, deve estabelecer e manter sistemas de informação, políticas e procedimentos adequados, tendo em vista, em especial, permitir que entidades importantes e essenciais e os respetivos fornecedores de redes e sistemas de informação divulguem e registem vulnerabilidades presentes nos produtos de TIC ou serviços de TIC, bem como proporcionar acesso às informações sobre vulnerabilidades constantes do registo a todas as partes interessadas. O registo deve incluir, em especial, informações que descrevam a vulnerabilidade, o produto de TIC ou os serviços de TIC afetados e a gravidade da vulnerabilidade em termos das circunstâncias em que pode ser explorada, a disponibilidade de correções e, na falta de correções, orientações destinadas aos utilizadores de produtos e serviços vulneráveis sobre formas de minimizar os riscos resultantes das vulnerabilidades divulgadas.

*Artigo 7.º*

***Quadros nacionais de gestão de crises de cibersegurança***

1. Os Estados-Membros devem designar uma ou várias autoridades competentes responsáveis pela gestão de incidentes e crises em grande escala. Os Estados-Membros devem igualmente certificar-se de que estas dispõem dos recursos necessários para desempenhar, de forma eficaz e eficiente, as suas funções.

2. Cada Estado-Membro deve identificar capacidades, ativos e procedimentos passíveis de utilização em caso de crise, para os efeitos da presente diretiva.

3. Cada Estado-Membro deve adotar um plano nacional de resposta a crises e incidentes de cibersegurança que estabeleça os objetivos e as modalidades de gestão de crises e incidentes de cibersegurança em grande escala. O plano deve estabelecer, concretamente, o seguinte:

   a) Objetivos das atividades e medidas nacionais de preparação;

   b) Atribuições e responsabilidades das autoridades nacionais competentes;

   c) Procedimentos de gestão de crises e canais de intercâmbio de informações;

   d) Medidas de preparação, incluindo exercícios e atividades de formação;

   e) Partes interessadas pertinentes dos setores público e privado e infraestruturas envolvidas;

   f) Procedimentos nacionais e acordos entre as autoridades e os organismos nacionais competentes para assegurar o apoio do Estado-Membro e a sua participação efetiva na gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível da União.

4. Os Estados-Membros devem comunicar à Comissão a designação das autoridades competentes a que se refere o n.º 1 e apresentar os respetivos planos nacionais de resposta a crises e incidentes de cibersegurança a que se refere o n.º 3 no prazo de três meses a contar da designação e da adoção desses planos. Os Estados-Membros podem excluir informações específicas do plano, na medida estritamente necessária para salvaguardar a sua segurança nacional.

*Artigo 8.º*

***Autoridades nacionais competentes e pontos de contacto únicos***

1. Cada Estado-Membro deve designar uma ou várias autoridades competentes responsáveis pela cibersegurança e pelo desempenho das funções de supervisão estabelecidas no capítulo VI da presente diretiva. Para esse efeito, os Estados-Membros podem designar uma ou várias autoridades existentes.

2. As autoridades competentes a que se refere o n.º 1 devem acompanhar a aplicação da presente diretiva a nível nacional.

3. Cada Estado-Membro deve designar um ponto de contacto único nacional para questões relacionadas com a cibersegurança (a seguir designado por «ponto de contacto único»). Caso um Estado-Membro designe apenas uma autoridade competente, esta é também o ponto de contacto único desse Estado-Membro.

4. Cada ponto de contacto único desempenha uma função de ligação para assegurar a cooperação transfronteiriça das autoridades do seu Estado-Membro com as autoridades competentes de outros Estados-Membros e para assegurar a cooperação transetorial com outras autoridades nacionais competentes do seu Estado-Membro.

5. Os Estados-Membros devem certificar-se de que as autoridades competentes a que se refere o n.º 1 e os pontos de contacto únicos dispõem de recursos adequados para desempenharem, de forma eficaz e eficiente, as suas funções e, desse modo, cumprirem os objetivos da presente diretiva. Os Estados-Membros devem garantir a

cooperação eficaz, eficiente e segura dos representantes designados no grupo de cooperação a que se refere o artigo 12.º.

6. Cada Estado-Membro deve notificar a Comissão, sem demora injustificada, da designação da autoridade competente a que se refere o n.º 1 e do ponto de contacto único a que se refere o n.º 3, das funções que lhes são atribuídas e de quaisquer alterações posteriores das mesmas. Cada Estado-Membro deve tornar pública a referida designação. A Comissão publica a lista dos pontos de contacto únicos designados.

*Artigo 9.º*

***Equipas de resposta a incidentes de segurança informática (CSIRT)***

1. Cada Estado-Membro deve designar uma ou várias CSIRT que cumpram os requisitos estabelecidos no artigo 10.º, n.º 1, abrangendo pelo menos os setores, subsetores ou entidades referidos nos anexos I e II, e que sejam responsáveis pelo tratamento de incidentes de acordo com um processo bem definido. As CSIRT podem ser criadas no seio de uma das autoridades competentes a que se refere o artigo 8.º.

2. Os Estados-Membros devem certificar-se de que cada CSIRT dispõe dos recursos adequados para desempenhar eficazmente as suas funções, tal como definidas no artigo 10.º, n.º 2.

3. Os Estados-Membros devem assegurar que cada CSIRT tenha ao seu dispor uma infraestrutura de informação e comunicação adequada, segura e resiliente para trocar informações com entidades essenciais e importantes e com outras partes interessadas. Para este efeito, devem garantir que as CSIRT contribuam para a implantação de ferramentas seguras de partilha de informações.

4. As CSIRT devem cooperar e, quando adequado, trocar informações importantes, em conformidade com o artigo 26.º, com comunidades setoriais ou transetoriais de confiança de entidades essenciais e importantes.

5. As CSIRT devem participar em análises pelos pares organizadas nos termos do artigo 16.º.

6. Os Estados-Membros devem garantir a cooperação eficaz, eficiente e segura das suas CSIRT no âmbito da rede de CSIRT a que se refere o artigo 13.º.

7. Os Estados-Membros devem comunicar à Comissão, sem demora injustificada, as CSIRT designadas nos termos do n.º 1, a CSIRT coordenadora designada nos termos do artigo 6.º, n.º 1, e as respetivas funções desempenhadas em relação às entidades a que se referem os anexos I e II.

8. Os Estados-Membros podem solicitar a assistência da ENISA na criação das CSIRT nacionais.

*Artigo 10.º*

***Requisitos e funções das CSIRT***

1. As CSIRT devem cumprir os seguintes requisitos:

a) As CSIRT devem garantir uma ampla disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais, e devem dispor de vários meios para contactar outras partes e para serem contactadas em qualquer momento. As CSIRT devem especificar claramente os canais de comunicação e divulgá-los junto da sua base de clientes e dos seus parceiros de cooperação;

b) As instalações das CSIRT e os seus sistemas de informação de apoio devem estar situados em locais seguros;

c) As CSIRT devem estar equipadas com um sistema adequado de gestão e encaminhamento de pedidos, sobretudo para facilitar transferências eficazes e eficientes;

d) As CSIRT devem dispor de pessoal suficiente para assegurar a sua disponibilidade em qualquer momento;

e) As CSIRT devem estar equipadas com sistemas redundantes e dispor de um espaço de trabalho de recurso para assegurar a continuidade dos seus serviços;

f) As CSIRT devem ter a possibilidade de participar em redes de cooperação internacional.

2. As funções das CSIRT são as seguintes:

a) Monitorizar ciberameaças, vulnerabilidades e incidentes a nível nacional;

b) Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às entidades essenciais e importantes, bem como a outras partes interessadas, sobre ciberameaças, vulnerabilidades e incidentes;

c) Intervir em caso de incidentes;

d) Proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança;

e) A pedido de uma entidade, realizar uma análise proativa da rede e dos sistemas de informação utilizados para a prestação dos seus serviços;

f) Participar na rede de CSIRT e prestar assistência mútua a outros membros da rede, a pedido destes.

3. As CSIRT devem estabelecer relações de cooperação com intervenientes do setor privado, com vista a alcançar da melhor forma os objetivos da diretiva.

4. A fim de facilitar a cooperação, as CSIRT devem promover a adoção e a utilização de práticas, sistemas de classificação e taxonomias comuns ou normalizadas em relação aos seguintes aspetos:

a) Procedimentos de tratamento de incidentes;

b) Gestão de crises de cibersegurança;

c) Divulgação coordenada de vulnerabilidades.

*Artigo 11.º*

***Cooperação a nível nacional***

1. Se forem entidades distintas, as autoridades competentes a que se refere o artigo 8.º, o ponto de contacto único e a(s) CSIRT do mesmo Estado-Membro devem cooperar entre si no que diz respeito ao cumprimento das obrigações previstas na presente diretiva.

2. Os Estados-Membros devem assegurar que as respetivas autoridades competentes ou as respetivas CSIRT recebem as notificações de incidentes, ciberameaças significativas e quase incidentes efetuadas nos termos da presente diretiva. Caso um Estado-Membro decida que as suas CSIRT não receberão as referidas notificações, estas devem ter acesso, na medida necessária ao desempenho das suas funções, aos dados sobre os incidentes notificados pelas entidades essenciais e importantes, nos termos do artigo 20.º.

3. Cada Estado-Membro deve certificar-se de que as respetivas autoridades competentes ou CSIRT informam o ponto de contacto único das notificações de incidentes, ciberameaças significativas e quase incidentes efetuadas nos termos da presente diretiva.

4. Na medida necessária ao desempenho das funções e ao cumprimento das obrigações estabelecidas na presente diretiva de forma eficaz, os Estados-Membros devem assegurar uma cooperação adequada entre as autoridades competentes e os pontos de contacto únicos e as autoridades policiais, as autoridades de proteção de dados, as autoridades responsáveis por infraestruturas críticas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] e as autoridades financeiras designadas em conformidade com o Regulamento (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[39] [Regulamento DORA] de cada Estado-Membro.

5. Os Estados-Membros devem garantir que as respetivas autoridades competentes fornecem regularmente às autoridades competentes designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] informações sobre riscos de cibersegurança, ciberameaças e incidentes que afetem entidades essenciais identificadas como críticas, ou como entidades equivalentes a entidades críticas, nos termos da referida diretiva, bem como sobre as medidas adotadas pelas autoridades competentes em resposta a esses riscos e incidentes.

[39] *[Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos]*.

## CAPÍTULO III

*Cooperação*

*Artigo 12.º*
***Grupo de cooperação***

1. É criado um grupo de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros no domínio de aplicação da diretiva.

2. O grupo de cooperação desempenha as suas funções com base nos programas de trabalho bienais a que se refere o n.º 6.

3. O grupo de cooperação é composto por representantes dos Estados-Membros, da Comissão e da ENISA. O Serviço Europeu para a Ação Externa participa nas atividades do grupo de cooperação na qualidade de observador. As autoridades europeias de supervisão (AES), em conformidade com o artigo 17.º, n.º 5, alínea c), do Regulamento (UE) XXXX/XXXX [Regulamento DORA], podem participar nas atividades do grupo de cooperação.

   Se for caso disso, o grupo de cooperação pode convidar representantes de partes interessadas relevantes para participar nos seus trabalhos.

   O secretariado do grupo é assegurado pela Comissão.

4. As funções do grupo de cooperação são as seguintes:

   a) Fornecer orientações às autoridades competentes sobre a transposição e aplicação da presente diretiva;

   b) Proceder ao intercâmbio de boas práticas e informações sobre a aplicação da presente diretiva, nomeadamente no que respeita a ciberameaças, incidentes, vulnerabilidades, quase incidentes, iniciativas de sensibilização, ações de formação, exercícios e competências, desenvolvimento das capacidades, normas e especificações técnicas;

   c) Trocar pareceres e cooperar com a Comissão em novas iniciativas políticas no domínio da cibersegurança;

   d) Trocar pareceres e cooperar com a Comissão em projetos de atos delegados ou de execução da Comissão adotados nos termos da presente diretiva;

   e) Proceder ao intercâmbio de boas práticas e informações com instituições, órgãos e organismos competentes da União;

   f) Discutir os relatórios das análises pelos pares a que se refere o artigo 16.º, n.º 7;

   g) Discutir os resultados das atividades conjuntas de supervisão em casos transfronteiriços, tal como referido no artigo 34.º;

   h) Fornecer orientações estratégicas à rede de CSIRT sobre questões emergentes específicas;

   i) Contribuir para as capacidades de cibersegurança em toda a União, facilitando o intercâmbio de funcionários nacionais no âmbito de um

programa de desenvolvimento das capacidades destinado ao pessoal das autoridades competentes ou das CSIRT dos Estados-Membros;

j) Organizar regularmente reuniões conjuntas com partes interessadas privadas de toda a União para discutir as atividades realizadas pelo grupo e partilhar pontos de vista sobre novos desafios políticos;

k) Discutir o trabalho desenvolvido em relação a exercícios de cibersegurança, incluindo o trabalho realizado pela ENISA.

5. O grupo de cooperação pode solicitar à rede de CSIRT um relatório técnico sobre determinados temas.

6. Até … [*24 meses após a data de entrada em vigor da presente diretiva*] e, daí em diante, de dois em dois anos, o grupo de cooperação deve elaborar um programa de trabalho relativo às ações a desenvolver para alcançar os seus objetivos e executar as suas funções. O calendário do primeiro programa adotado ao abrigo da presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148.

7. A Comissão pode adotar atos de execução que estabeleçam as disposições processuais necessárias ao funcionamento do grupo de cooperação. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2.

8. O grupo de cooperação reúne-se regularmente, pelo menos uma vez por ano, com o grupo para a resiliência das entidades críticas criado ao abrigo da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas], com vista a promover a cooperação estratégica e o intercâmbio de informações.

*Artigo 13.º*
***Rede de CSIRT***

1. É criada uma rede de CSIRT nacionais para contribuir para o desenvolvimento da confiança e promover uma cooperação operacional célere e eficaz entre os Estados-Membros.

2. A rede de CSIRT é composta por representantes das CSIRT dos Estados-Membros e da CERT-UE. A Comissão participa na rede de CSIRT na qualidade de observadora. A ENISA assegura os serviços de secretariado e apoia ativamente a cooperação entre as CSIRT.

3. As funções da rede de CSIRT são as seguintes:

a) Proceder ao intercâmbio de informações sobre as capacidades das CSIRT;

b) Proceder ao intercâmbio de informações importantes sobre incidentes, quase incidentes, ciberameaças, riscos e vulnerabilidades;

c) A pedido de um representante da rede de CSIRT potencialmente afetado por um incidente, trocar e discutir informações relacionadas com esse incidentes e com ciberameaças, riscos e vulnerabilidades conexas;

d) A pedido de um representante da rede de CSIRT, discutir e, se possível, aplicar uma resposta coordenada a um incidente identificado no âmbito da jurisdição desse Estado-Membro;

e) Prestar apoio aos Estados-Membros no tratamento de incidentes transfronteiriços nos termos da presente diretiva;

f) Cooperar e prestar assistência às CSIRT designadas nos termos do artigo 6.º relativamente à gestão da divulgação coordenada de vulnerabilidades que afetem vários fabricantes ou fornecedores de produtos de TIC, serviços de TIC e processos de TIC estabelecidos em Estados-Membros diferentes;

g) Discutir e identificar outras formas de cooperação operacional, nomeadamente no que se refere:

i) às categorias de ciberameaças e incidentes,

ii) aos alertas rápidos,

iii) à assistência mútua,

iv) aos princípios e às formas de coordenação na resposta a riscos e incidentes de dimensão transfronteiriça,

v) ao contributo para o plano nacional de resposta a crises e incidentes de cibersegurança a que se refere o artigo 7.º, n.º 3;

h) Informar o grupo de cooperação sobre as suas atividades e sobre as outras formas de cooperação operacional discutidas nos termos da alínea g), solicitando, quando necessário, orientações a esse respeito;

i) Analisar os resultados dos exercícios de cibersegurança, incluindo os exercícios organizados pela ENISA;

j) A pedido de determinada CSIRT, discutir as suas capacidades e o seu grau de preparação;

k) Cooperar e trocar informações com centros de operações de segurança regionais e a nível da União, a fim de melhorar o conhecimento situacional comum em matéria de incidentes e ameaças em toda a União;

l) Discutir os relatórios das análises pelos pares a que se refere o artigo 16.º, n.º 7;

m) Emitir orientações a fim de facilitar a convergência das práticas operacionais no que diz respeito à aplicação do disposto no presente artigo em matéria de cooperação operacional.

4. Para efeitos da avaliação a que se refere o artigo 35.º e até [*24 meses após a data de entrada em vigor da presente diretiva*] e, daí em diante, de dois em dois anos, a rede de CSIRT deve avaliar os progressos alcançados no domínio da cooperação operacional e apresentar um relatório. Em especial, o relatório deve expor conclusões sobre os resultados das análises pelos pares realizadas nos termos do artigo 16.º em relação às CSIRT nacionais, incluindo conclusões e recomendações nos termos do referido artigo. Esse relatório deve ser apresentado também ao grupo de cooperação.

5. A rede de CSIRT adota o seu próprio regulamento interno.

*Artigo 14.º*

***Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe)***

1. É criada a Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional e para assegurar o intercâmbio regular de informações entre os Estados-Membros e as instituições, órgãos e organismos da União.

2. A UE-CyCLONe é constituída pelos representantes das autoridades de gestão de crises dos Estados-Membros designadas nos termos do artigo 7.º, pela Comissão e pela ENISA. A ENISA assegura os serviços de secretariado da rede e presta apoio ao intercâmbio seguro de informações.

3. As funções da UE-CyCLONe são as seguintes:

   a) Aumentar o nível de preparação para a gestão de incidentes e crises em grande escala;

   b) Desenvolver um conhecimento situacional comum sobre eventos de cibersegurança significativos;

   c) Coordenar a gestão de incidentes e crises em grande escala e apoiar a tomada de decisões a nível político em relação a tais incidentes e crises;

   d) Discutir os planos nacionais de resposta a crises e incidentes de cibersegurança a que se refere o artigo 7.º, n.º 2;

4. A UE-CyCLONe adota o seu regulamento interno.

5. A UE-CyCLONe presta regularmente informações ao grupo de cooperação sobre ciberameaças, incidentes e tendências, dedicando especial atenção ao seu impacto em entidades essenciais e importantes.

6. A UE-CyCLONe coopera com a rede de CSIRT com base em disposições processuais acordadas.

*Artigo 15.º*

***Relatório sobre o estado da cibersegurança na União***

1. A ENISA deve elaborar, em cooperação com a Comissão, um relatório bienal sobre o estado da cibersegurança na União. Este relatório deve, nomeadamente, incluir uma análise dos seguintes aspetos:

   a) O desenvolvimento das capacidades de cibersegurança em toda a União;

   b) Os recursos técnicos, financeiros e humanos ao dispor das autoridades competentes e afetos à execução das políticas de cibersegurança, e a aplicação de medidas de supervisão e de medidas coercivas à luz dos resultados das análises pelos pares a que se refere o artigo 16.º;

   c) Um índice de cibersegurança que contemple uma avaliação agregada do nível de maturidade das capacidades de cibersegurança.

2. O relatório deve incluir recomendações políticas específicas para aumentar o nível de cibersegurança em toda a União e um resumo das constatações, para o período em questão, dos relatórios sobre a situação técnica da cibersegurança na UE elaborados pela ENISA em conformidade com o artigo 7.º, n.º 6, do Regulamento (UE) 2019/881.

*Artigo 16.º*

**Análises pelos pares**

1. Após consulta do grupo de cooperação e da ENISA e, o mais tardar, 18 meses após a entrada em vigor da presente diretiva, a Comissão estabelece a metodologia e o conteúdo de um sistema de análises pelos pares destinado a avaliar a eficácia das políticas de cibersegurança dos Estados-Membros. As análises devem ser realizadas por peritos técnicos em cibersegurança provenientes de Estados-Membros diferentes do Estado-Membro avaliado e devem incidir, no mínimo, nos seguintes aspetos:

   i) a eficácia da aplicação dos requisitos de gestão dos riscos de cibersegurança e das obrigações de notificação a que se referem os artigos 18.º e 20.º,

   ii) o nível de capacidades, incluindo os recursos financeiros, técnicos e humanos disponíveis, e a eficácia das autoridades nacionais competentes no desempenho das suas funções,

   iii) as capacidades operacionais e a eficácia das CSIRT,

   iv) a eficácia da assistência mútua a que se refere o artigo 34.º,

   v) a eficácia do quadro de partilha de informações a que se refere o artigo 26.º da presente diretiva.

2. A metodologia deve incluir critérios objetivos, não discriminatórios, equitativos e transparentes com base nos quais os Estados-Membros designarão os peritos elegíveis para realizarem as análises pelos pares. A ENISA e a Comissão designam peritos para participarem nas análises pelos pares na qualidade de observadores. Com o apoio da ENISA, a Comissão estabelece, no âmbito da metodologia a que se refere o n.º 1, um sistema objetivo, não discriminatório, equitativo e transparente para a seleção e distribuição aleatória de peritos para cada análise pelos pares.

3. Os aspetos organizativos das análises pelos pares são decididos pela Comissão, apoiada pela ENISA e após consulta do grupo de cooperação, e devem basear-se nos critérios definidos na metodologia a que se refere o n.º 1. As análises pelos pares devem avaliar os aspetos mencionados no n.º 1 no atinente a todos os Estados-Membros e setores, incluindo questões especificamente relacionadas com um ou vários Estados-Membros ou um ou vários setores.

4. As análises pelos pares devem incluir visitas virtuais ou físicas aos locais e discussões fora do local. Tendo em conta o princípio da boa cooperação, os Estados-Membros objeto da análise devem facultar aos peritos designados as informações solicitadas que sejam necessárias para a avaliação dos aspetos em análise. As informações obtidas durante o processo de análise pelos pares devem ser utilizadas exclusivamente para esse fim. Os peritos que participam na análise pelos pares não podem divulgar a terceiros quaisquer informações sensíveis ou confidenciais obtidas no decurso da referida análise.

5. Os aspetos que tenham sido analisados num Estado-Membro não serão objeto de uma nova análise pelos pares nesse Estado-Membro nos dois anos seguintes, salvo decisão em contrário da Comissão, após consulta da ENISA e do grupo de cooperação.

6. O Estado-Membro deve assegurar que qualquer risco de conflito de interesses respeitante aos peritos designados é revelado, sem demora injustificada, aos outros Estados-Membros, à Comissão e à ENISA.

7. Os peritos que participam nas análises pelos pares devem elaborar relatórios sobre as constatações e conclusões dessas análises. Os relatórios devem ser apresentados à Comissão, ao grupo de cooperação, à rede de CSIRT e à ENISA. Os relatórios devem ser discutidos no seio do grupo de cooperação e da rede de CSIRT. Os relatórios podem ser publicados no sítio Web do grupo de cooperação.

## CAPÍTULO IV

### *Obrigações de gestão dos riscos de cibersegurança e de notificação*

### SECÇÃO I

*Gestão dos riscos de cibersegurança e notificação*

#### *Artigo 17.º*

#### *Governação*

1. Os Estados-Membros devem assegurar que os órgãos de direção das entidades essenciais e importantes aprovam as medidas de gestão dos riscos de cibersegurança tomadas por essas entidades em cumprimento do disposto no artigo 18.º, supervisionam a sua aplicação e são responsabilizados em caso de incumprimento das obrigações estabelecidas no referido artigo por parte das referidas entidades.
2. Compete igualmente aos Estados-Membros garantir que os membros do órgão de direção frequentam regularmente ações de formação específicas, a fim de adquirirem conhecimentos e competências suficientes para compreenderem e avaliarem os riscos de segurança e as práticas de gestão, bem como o seu impacto nas operações da entidade.

#### *Artigo 18.º*

#### *Medidas de gestão dos riscos de cibersegurança*

1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes tomam medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam na prestação dos seus serviços. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.
2. As medidas referidas no n.º 1 devem abranger, pelo menos, os seguintes aspetos:
   a) Políticas de análise dos riscos e de segurança dos sistemas de informação;
   b) Tratamento de incidentes (prevenção, deteção e resposta a incidentes);
   c) Gestão de crises e da continuidade das atividades;

d) Segurança da cadeia de fornecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços, tais como os prestadores de serviços de armazenamento e tratamento de dados ou serviços de segurança geridos;

e) Segurança na aquisição, desenvolvimento e manutenção das redes e dos sistemas de informação, incluindo o tratamento e a divulgação de vulnerabilidades;

f) Políticas e procedimentos (testes e auditoria) para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;

g) A utilização de criptografia e cifragem.

3. Os Estados-Membros devem garantir que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), as entidades têm em conta as vulnerabilidades específicas de cada fornecedor e cada prestador de serviços, bem como a qualidade global dos produtos e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro.

4. Os Estados-Membros devem assegurar que, caso uma entidade conclua que os seus serviços ou as suas atribuições não estão em conformidade com os requisitos estabelecidos no n.º 2, esta toma todas as medidas corretivas necessárias, sem demora injustificada, para assegurar a conformidade do serviço em causa.

5. A Comissão pode adotar atos de execução para definir as especificações técnicas e metodológicas dos elementos a que se refere o n.º 2. Na preparação desses atos, a Comissão segue o procedimento de exame a que se refere o artigo 37.º, n.º 2, e cumpre, tanto quanto possível, normas internacionais e europeias, bem como as especificações técnicas aplicáveis.

6. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 36.º para completar os elementos estabelecidos no n.º 2, a fim de ter em conta novas ciberameaças, avanços tecnológicos ou especificidades setoriais.

*Artigo 19.º*

***Avaliações coordenadas a nível da UE dos riscos de cadeias de fornecimento críticas***

1. Em cooperação com a Comissão e a ENISA, o grupo de cooperação pode realizar avaliações coordenadas dos riscos de segurança de cadeias de fornecimento de produtos, sistemas ou serviços de TIC críticos, tendo em conta fatores de risco de natureza técnica e, quando pertinente, de natureza não técnica.

2. Após consulta do grupo de cooperação e da ENISA, a Comissão deve identificar os produtos, sistemas ou serviços de TIC críticos específicos que podem ser sujeitos à avaliação coordenada dos riscos a que se refere o n.º 1.

*Artigo 20.º*

***Obrigações de notificação***

1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam as autoridades competentes ou a CSIRT, sem demora injustificada e nos termos dos n.os 3 e 4, de qualquer incidente que tenha um impacto significativo na prestação dos seus serviços. Quando pertinente, essas entidades devem notificar os destinatários dos seus serviços, sem demora injustificada, de incidentes suscetíveis de afetar negativamente a prestação desse serviço. Compete aos Estados-Membros garantir que as referidas entidades comunicam, entre outras, quaisquer informações que permitam às autoridades competentes ou à CSIRT determinar o eventual impacto transfronteiriço do incidente.

2. Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam as autoridades competentes ou a CSIRT, sem demora injustificada, de qualquer ciberameaça significativa identificada por essas entidades que pudesse ter dado origem a um incidente significativo.

   Quando for o caso, as referidas entidades devem notificar, sem demora injustificada, os destinatários dos seus serviços potencialmente afetados por uma ciberameaça significativa das medidas proativas ou corretivas que estes podem tomar para responder a essa ameaça. Quando pertinente, as entidades devem igualmente notificar os referidos destinatários da própria ameaça. A notificação não acarreta responsabilidades acrescidas para a entidade notificadora.

3. Considera-se que um incidente é significativo se:

   a) Tiver causado ou for suscetível de causar perturbações operacionais ou perdas financeiras substanciais à entidade em causa;

   b) Tiver afetado ou for suscetível de afetar outras pessoas singulares ou coletivas, causando perdas materiais ou não materiais consideráveis.

4. Os Estados-Membros devem garantir que, para efeitos da notificação prevista no n.º 1, as entidades em causa apresentam às autoridades competentes ou à CSIRT:

   a) Sem demora injustificada e, em qualquer caso, no prazo de 24 horas depois de terem tomado conhecimento do incidente, uma notificação inicial que, se for o caso, deve indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso;

   b) A pedido de uma autoridade competente ou de uma CSIRT, um relatório intercalar com informações atualizadas importantes sobre a situação;

   c) O mais tardar um mês após a notificação mencionada na alínea a), um relatório final que contenha, no mínimo, os seguintes elementos:

      i) uma descrição pormenorizada do incidente, da sua gravidade e do seu impacto,

      ii) o tipo de ameaça ou provável causa primária do incidente,

      iii) medidas de atenuação aplicadas e em curso.

   Os Estados-Membros devem estabelecer que, em casos devidamente justificados e com a concordância das autoridades competentes ou da CSIRT, a entidade em causa poderá não cumprir os prazos estabelecidos nas alíneas a) e c).

5. No prazo de 24 horas após a receção da notificação inicial a que se refere o n.º 4, alínea a), as autoridades nacionais competentes ou a CSIRT devem apresentar uma resposta à entidade notificadora que forneça, designadamente, as suas observações

iniciais sobre o incidente e, a pedido da entidade, orientações sobre a aplicação de possíveis medidas de atenuação. Nos casos em que a CSIRT não tenha recebido a notificação a que se referem o n.º 1, as orientações devem ser fornecidas pela autoridade competente, em colaboração com a CSIRT. A CSIRT deve prestar apoio técnico adicional, caso a entidade em causa o solicite. Nos casos em que se suspeite da natureza criminosa do incidente, as autoridades nacionais competentes ou a CSIRT devem fornecer igualmente orientações sobre a notificação do incidente às autoridades policiais.

6. Quando pertinente, e em particular se o incidente a que se refere o n.º 1 disser respeito a dois ou mais Estados-Membros, a autoridade competente ou a CSIRT deve informar os outros Estados-Membros afetados e a ENISA do incidente. Ao fazê-lo, as autoridades competentes, as CSIRT e os pontos de contacto únicos devem salvaguardar, de acordo com o direito da União ou com a legislação nacional conforme com o direito da União, a segurança e os interesses comerciais da entidade, bem como a confidencialidade das informações prestadas.

7. Nos casos em que seja necessário sensibilizar o público para evitar um incidente ou para responder a um incidente em curso, ou em que a divulgação do incidente seja de interesse público, a autoridade competente ou a CSIRT e, se for o caso, as autoridades ou as CSIRT dos outros Estados-Membros afetados podem, após consulta da entidade em causa, informar o público do incidente ou exigir que a entidade o faça.

8. A pedido da autoridade competente ou da CSIRT, o ponto de contacto único deve transmitir as notificações recebidas nos termos dos n.os 1 e 2 aos pontos de contacto únicos dos outros Estados-Membros afetados.

9. O ponto de contacto único deve apresentar mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre os incidentes, as ciberameaças significativas e os quase incidentes notificados nos termos dos n.os 1 e 2 e do artigo 27.º A fim de contribuir para a comparabilidade das informações apresentadas, a ENISA pode emitir orientações técnicas sobre os parâmetros das informações a incluir no relatório de síntese.

10. As autoridades competentes devem fornecer às autoridades competentes designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] informações sobre os incidentes e as ciberameaças notificadas nos termos dos n.os 1 e 2 por entidades essenciais identificadas como entidades críticas, ou por entidades equivalentes a entidades críticas, nos termos da diretiva supramencionada.

11. A Comissão pode adotar atos de execução que especifiquem o tipo de informações, o formato e o procedimento das notificações apresentadas nos termos dos n.os 1 e 2. A Comissão pode ainda adotar atos de execução que especifiquem os casos em que um incidente deve ser considerado significativo, conforme referido no n.º 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2.

*Artigo 21.º*

***Utilização dos sistemas europeus de certificação da cibersegurança***

1. A fim de demonstrar o cumprimento de certos requisitos estabelecidos no artigo 18.º, os Estados-Membros podem exigir que as entidades essenciais e importantes certifiquem determinados produtos de TIC, serviços de TIC e processos de TIC no âmbito de sistemas europeus de certificação da cibersegurança específicos adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881. Os produtos, serviços e processos sujeitos a certificação podem ser desenvolvidos por uma entidade essencial ou importante ou ser adquiridos a terceiros.

2. A Comissão fica habilitada a adotar atos delegados que especifiquem as categorias de entidades essenciais obrigadas a obter um certificado e os sistemas europeus de certificação da cibersegurança a que devem recorrer para o efeito nos termos do n.º 1. Os atos delegados são adotados em conformidade com o artigo 36.º.

3. A Comissão pode solicitar à ENISA a elaboração de um projeto de sistema nos termos do artigo 48.º, n.º 2, do Regulamento (UE) 2019/881 nos casos em que não exista um sistema europeu de certificação da cibersegurança adequado para os efeitos do n.º 2.

*Artigo 22.º*

***Normalização***

1. A fim de promover a aplicação convergente do artigo 18.º, n.os 1 e 2, os Estados-Membros devem incentivar, sem imporem ou discriminarem em favor da utilização de um determinado tipo de tecnologia, a utilização de normas e especificações europeias ou internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação.

2. A ENISA deve formular, em colaboração com os Estados-Membros, recomendações e orientações sobre os domínios técnicos que devem ser considerados no âmbito do n.º 1, bem como sobre as normas já existentes, incluindo as normas nacionais dos Estados-Membros, que permitiriam abranger esses domínios.

*Artigo 23.º*

***Bases de dados dos nomes de domínio e dos dados de registo***

1. Com vista a contribuir para a segurança, a estabilidade e a resiliência do DNS, os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos recolhem e mantêm dados exatos e completos relativos ao registo de nomes de domínio numa base de dados específica, com a devida diligência, em conformidade com a legislação da União em matéria de proteção de dados no que respeita aos dados pessoais.

2. Os Estados-Membros devem assegurar que as bases de dados relativos ao registo de nomes de domínio a que se refere o n.º 1 contêm as informações necessárias para identificar e contactar os titulares dos nomes de domínio e os pontos de contacto que administram os nomes de domínio sob o domínio de topo.

3. Os Estados-Membros devem ainda garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos dispõem de políticas e procedimentos para assegurar que as bases de dados contêm

informações exatas e completas. Os Estados-Membros devem certificar-se de que essas políticas e procedimentos são tornados públicos.

4. Os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos publicam, sem demora injustificada após o registo de um nome de domínio, os dados relativos ao registo do domínio que não sejam dados pessoais.

5. Os Estados-Membros devem assegurar que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos concedem acesso a dados específicos relativos ao registo de nomes de domínio aos requerentes legítimos de acesso que apresentem um pedido lícito e devidamente justificado, em conformidade com a legislação da União em matéria de proteção de dados. Os Estados-Membros devem assegurar que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos respondem a todos os pedidos de acesso sem demora injustificada. Compete aos Estados-Membros garantir que as políticas e procedimentos de divulgação dos referidos dados são tornados públicos.

Secção II

**Competência e registo**

*Artigo 24.º*

***Competência e territorialidade***

1. Considera-se que os prestadores de serviços de DNS, os registos de nomes de domínio de topo, os prestadores de serviços de computação em nuvem, os prestadores de serviços de centro de dados e os fornecedores de redes de distribuição de conteúdos referidos no anexo I, ponto 8, bem como os prestadores de serviços digitais referidos no anexo II, ponto 6, estão sob a jurisdição do Estado-Membro em que têm o seu estabelecimento principal na União.

2. Para efeitos da presente diretiva, considera-se que as entidades referidas no n.º 1 têm o seu estabelecimento principal na União no Estado-Membro em que são tomadas as decisões relacionadas com as medidas de gestão dos riscos de cibersegurança. Se tais decisões não forem tomadas num estabelecimento situado na União, considera-se que o estabelecimento principal se situa no Estado-Membro em que as entidades têm o estabelecimento com o maior número de trabalhadores na União.

3. Se uma entidade referida no n.º 1 não estiver estabelecida na União, mas aí oferecer serviços, deve designar um representante na União. O representante deve estar estabelecido num dos Estados-Membros em que os serviços são oferecidos. Considera-se que tal entidade está sob a jurisdição do Estado-Membro em que o representante está estabelecido. Na ausência de um representante designado na União nos termos do presente artigo, qualquer Estado-Membro em que a entidade preste serviços pode intentar ações judiciais contra essa entidade por incumprimento das obrigações decorrentes da presente diretiva.

4. A designação de um representante por parte de uma entidade referida no n.º 1 não prejudica as ações judiciais que possam ser intentadas contra a própria entidade.

*Artigo 25.º*

***Registo de entidades essenciais e importantes***

1. A ENISA deve criar e manter um registo das entidades essenciais e importantes referidas no artigo 24.º, n.º 1. As entidades devem fornecer as seguintes informações à ENISA até [o mais tardar 12 meses após a entrada em vigor da diretiva]:

   a) Nome da entidade;

   b) Endereço do seu estabelecimento principal e dos outros estabelecimentos legais que possui na União ou, se não estiver estabelecida na União, do seu representante designado nos termos do artigo 24.º, n.º 3;

   c) Contactos atualizados, incluindo endereços de correio eletrónico e números de telefone das entidades.

2. As entidades referidas no n.º 1 devem notificar a ENISA de quaisquer alterações dos dados que forneceram nos termos do n.º 1, sem demora e, em qualquer caso, no prazo de três meses a contar da data em que a alteração produziu efeitos.

3. Após a receção das informações referidas no n.º 1, a ENISA deve transmiti-las aos pontos de contacto únicos em função da localização indicada do estabelecimento principal de cada entidade ou, no caso das que não estejam estabelecidas na União, do seu representante designado. Caso uma entidade referida no n.º 1 possua, além do seu estabelecimento principal na União, outros estabelecimentos noutros Estados-Membros, a ENISA deve informar também os pontos de contacto únicos desses Estados-Membros.

4. Se uma entidade não registar a sua atividade ou não fornecer as informações exigidas dentro do prazo estabelecido no n.º 1, qualquer Estado-Membro onde a entidade preste serviços tem competência para assegurar o cumprimento das obrigações estabelecidas na presente diretiva por parte dessa entidade.

## CAPÍTULO V

## *Partilha de informações*

*Artigo 26.º*

***Acordos de partilha de informações sobre cibersegurança***

1. Sem prejuízo do Regulamento (UE) 2016/679, os Estados-Membros devem assegurar que as entidades essenciais e importantes podem proceder ao intercâmbio de informações pertinentes sobre cibersegurança, nomeadamente relacionadas com ciberameaças, vulnerabilidades, indicadores de exposição a riscos, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração, desde que tal partilha de informações:

   a) Tenha como objetivo evitar, detetar e dar resposta a incidentes ou atenuá-los;

   b) Reforce o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação e apoiar um leque de capacidades defensivas, a correção e divulgação de

vulnerabilidades, as técnicas de deteção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação.

2. Os Estados-Membros devem assegurar que o intercâmbio de informações ocorre no seio de comunidades de confiança de entidades essenciais e importantes. Tal intercâmbio deve ser executado mediante acordos de partilha de informações que protejam a natureza potencialmente sensível das informações partilhadas e sejam conformes com as regras do direito da União a que se refere o n.º 1.

3. Os Estados-Membros devem definir regras que especifiquem o procedimento, os elementos operacionais (incluindo a utilização de plataformas TIC dedicadas), o teor e as condições dos acordos de partilha de informações a que se refere o n.º 2. Tais regras devem também definir os pormenores do envolvimento das autoridades públicas nesses acordos, bem como os elementos operacionais, incluindo a utilização de plataformas TIC dedicadas. Os Estados-Membros devem oferecer apoio à aplicação de tais acordos, em conformidade com as suas políticas a que se refere o artigo 5.º, n.º 2, alínea g).

4. As entidades essenciais e importantes devem notificar as autoridades competentes da sua participação nos acordos de partilha de informações referidos no n.º 2, aquando da sua celebração, ou, quando aplicável, da sua retirada de tais acordos, assim que esta produza efeitos.

5. Em conformidade com a legislação da União, a ENISA deve apoiar a celebração dos acordos de partilha de informações sobre cibersegurança referidos no n.º 2, fornecendo documentos de boas práticas e orientações.

*Artigo 27.º*

***Notificação voluntária de informações pertinentes***

Sem prejuízo do disposto no artigo 3.º, os Estados-Membros devem assegurar que as entidades não abrangidas pelo âmbito da presente diretiva podem apresentar notificações, a título voluntário, de incidentes significativos, ciberameaças ou quase incidentes. No tratamento das notificações, os Estados-Membros devem aplicar o procedimento previsto no artigo 20.º. Os Estados-Membros podem dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias. A notificação voluntária não pode dar origem à imposição de quaisquer obrigações adicionais à entidade notificadora, às quais não estaria sujeita se não tivesse apresentado a notificação.

## CAPÍTULO VI

*Supervisão e execução coerciva*

*Artigo 28.º*

***Aspetos gerais relativos à supervisão e execução coerciva***

1. Os Estados-Membros devem assegurar que as autoridades competentes controlam eficazmente o cumprimento da presente diretiva e tomam as medidas necessárias para garantir esse cumprimento, em especial das obrigações previstas nos artigos 18.º e 20.º.

2. Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita colaboração com as autoridades encarregadas da proteção de dados.

*Artigo 29.º*

**Supervisão e execução coerciva no respeitante a entidades essenciais**

1. Os Estados-Membros devem assegurar que as medidas de supervisão ou coercivas impostas às entidades essenciais no que respeita às obrigações previstas na presente diretiva são efetivas, proporcionadas e dissuasivas, tendo em conta as circunstâncias de cada caso concreto.

2. Os Estados-Membros devem assegurar que, no exercício das suas funções de supervisão em relação a entidades essenciais, as autoridades competentes dispõem de poderes para submeter essas entidades a:

   a) Inspeções no local e supervisão remota, incluindo controlos aleatórios;

   b) Auditorias regulares;

   c) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos;

   d) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes;

   e) Pedidos de informações necessárias para avaliar as medidas de cibersegurança adotadas pela entidade, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de notificar a ENISA nos termos do artigo 25.º, n.os 1 e 2;

   f) Pedidos de acesso a dados, documentos ou quaisquer informações necessárias para o desempenho das suas funções de supervisão;

   g) Pedidos de provas da aplicação das políticas de cibersegurança, como os resultados de auditorias de segurança efetuadas por um auditor qualificado e os respetivos elementos de prova subjacentes.

3. Ao exercerem os poderes previstos no n.º 2, alíneas e) a g), as autoridades competentes devem indicar a finalidade do pedido e especificar as informações solicitadas.

4. Os Estados-Membros devem assegurar que, no exercício dos seus poderes de execução coerciva em relação a entidades essenciais, as autoridades competentes dispõem de poderes para:

   a) Emitir advertências sobre o não cumprimento, por parte das entidades, das obrigações previstas na presente diretiva;

   b) Emitir instruções vinculativas ou uma ordem que exija que essas entidades corrijam as deficiências detetadas ou as infrações às obrigações previstas na presente diretiva;

   c) Ordenar que essas entidades cessem condutas não conformes com as obrigações previstas na presente diretiva e se abstenham de as repetir;

d) Ordenar que essas entidades garantam a conformidade das suas medidas de gestão dos riscos e/ou obrigações de notificação com as obrigações estabelecidas nos artigos 18.º e 20.º de uma forma e num período especificados;

e) Ordenar que essas entidades informem as pessoas singulares ou coletivas a quem prestam serviços ou atividades que sejam potencialmente afetadas por uma ciberameaça significativa de quaisquer possíveis medidas de proteção ou corretivas que possam ser tomadas por essas pessoas em resposta a essa ameaça;

f) Ordenar que essas entidades apliquem, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança;

g) Designar um supervisor com funções bem definidas durante um determinado período para supervisionar o cumprimento das obrigações previstas nos artigos 18.º e 20.º;

h) Ordenar que essas entidades tornem públicos os aspetos do não cumprimento das obrigações estabelecidas na presente diretiva de uma determinada forma;

i) Fazer uma declaração pública que identifique as pessoas singulares e coletivas responsáveis pela violação de uma obrigação prevista na presente diretiva e a natureza dessa violação;

j) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, de acordo com a legislação nacional, de uma coima nos termos do artigo 31.º, em complemento ou em vez das medidas referidas nas alíneas a) a i) do presente número, em função das circunstâncias de cada caso concreto.

5. Sempre que as medidas coercivas adotadas nos termos do n.º 4, alíneas a) a d) e f), se revelem ineficazes, os Estados-Membros devem assegurar que as autoridades competentes dispõem de poderes para estabelecer um prazo dentro do qual se solicita à entidade essencial que tome as medidas necessárias para corrigir as deficiências ou cumprir os requisitos dessas autoridades. Se a medida solicitada não for tomada dentro do prazo estabelecido, os Estados-Membros devem assegurar que as autoridades competentes dispõem de poderes para:

a) Suspender ou solicitar a um organismo de certificação ou autorização a suspensão de uma certificação ou autorização relativa a uma parte ou à totalidade dos serviços ou atividades prestadas por uma entidade essencial;

b) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, de acordo com a legislação nacional, de uma proibição temporária de exercer funções de gestão nessa entidade essencial contra qualquer pessoa com responsabilidades de gestão a nível de diretor executivo ou representante legal e qualquer outra pessoa singular considerada responsável pela violação.

Estas sanções só são aplicadas até a entidade tomar as medidas necessárias para corrigir as deficiências ou cumprir os requisitos da autoridade competente responsável pela aplicação dessas sanções.

6. Os Estados-Membros devem assegurar que qualquer pessoa singular responsável por uma entidade essencial ou que atue como representante da mesma, com base no poder de a representar, na autoridade para tomar decisões em seu nome, ou na autoridade para exercer o controlo da mesma, dispõe de poderes para assegurar o seu

cumprimento das obrigações previstas na presente diretiva. Os Estados-Membros devem assegurar que essas pessoas singulares podem ser consideradas responsáveis pela violação dos seus deveres de assegurar o cumprimento das obrigações previstas na presente diretiva.

7. Ao tomarem qualquer uma das medidas coercivas ou aplicarem quaisquer sanções nos termos dos n.os 4 e 5, as autoridades competentes devem respeitar os direitos da defesa e ponderar as circunstâncias de cada caso concreto e, no mínimo, ter em devida conta:

   a) A gravidade da infração e a importância das disposições violadas. Entre as infrações que devem ser consideradas graves encontram-se: violações repetidas, não notificação ou não correção de incidentes com um efeito perturbador importante, não correção de deficiências na sequência de instruções vinculativas das autoridades competentes, obstrução de auditorias ou atividades de acompanhamento ordenadas pela autoridade competente na sequência da constatação de uma infração, prestação de informações falsas ou grosseiramente inexatas em relação aos requisitos de gestão dos riscos ou às obrigações de notificação estabelecidas nos artigos 18.º e 20.º;

   b) A duração da infração, incluindo o elemento de infrações repetidas;

   c) Os danos efetivamente causados ou as perdas efetivamente sofridas, ou potenciais danos ou perdas que poderiam ter sido desencadeados, na medida em que possam ser determinados. Ao avaliar este aspeto, devem ser tidos em conta, nomeadamente, os prejuízos financeiros ou económicos efetivos ou potenciais, os efeitos noutros serviços, o número de utilizadores afetados ou potencialmente afetados;

   d) O caráter doloso ou negligente da infração;

   e) As medidas tomadas pela entidade para prevenir ou atenuar os danos e/ou perdas;

   f) O cumprimento de códigos de conduta ou procedimentos de certificação aprovados;

   g) O nível de cooperação das pessoas singulares ou coletivas consideradas responsáveis com as autoridades competentes.

8. As autoridades competentes devem apresentar uma fundamentação pormenorizada das suas decisões de aplicação de medidas coercivas. Antes de tomarem tais decisões, as autoridades competentes devem notificar as entidades em causa das suas conclusões preliminares e conceder um prazo razoável para que essas entidades apresentem as suas observações.

9. Os Estados-Membros devem assegurar que as suas autoridades competentes informam as autoridades competentes do Estado-Membro em causa designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas], quando exercem os seus poderes de supervisão e de execução coerciva com vista a assegurar o cumprimento das obrigações decorrentes da presente diretiva por parte de uma entidade essencial identificada como crítica, ou como entidade equivalente a uma entidade crítica, nos termos da diretiva supramencionada. A pedido das autoridades competentes ao abrigo da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas], as autoridades competentes podem

exercer os seus poderes de supervisão e execução coerciva sobre uma entidade essencial identificada como crítica ou equivalente.

*Artigo 30.º*

**Supervisão e execução coerciva no respeitante a entidades importantes**

1. Sempre que lhes sejam apresentadas provas ou indícios de que uma entidade importante não está a cumprir as obrigações previstas na presente diretiva, em especial nos artigos 18.º e 20.º, os Estados-Membros devem assegurar que as autoridades competentes atuam em conformidade, se necessário, tomando medidas de supervisão *ex post*.

2. Os Estados-Membros devem assegurar que, no exercício das suas funções de supervisão em relação a entidades importantes, as autoridades competentes dispõem de poderes para submeter essas entidades a:

   a) Inspeções no local e supervisão *ex post* remota;

   b) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos;

   c) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, equitativos e transparentes;

   d) Pedidos de quaisquer informações necessárias para avaliar *ex post* as medidas de cibersegurança, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de notificar a ENISA nos termos do artigo 25.º, n.os 1 e 2;

   e) Pedidos de acesso a dados, documentos e/ou quaisquer informações necessárias para o desempenho das funções de supervisão.

3. Ao exercerem os poderes previstos no n.º 2, alíneas d) ou e), as autoridades competentes devem indicar a finalidade do pedido e especificar as informações solicitadas.

4. Os Estados-Membros devem assegurar que, no exercício dos seus poderes de execução coerciva em relação a entidades importantes, as autoridades competentes dispõem de poderes para:

   a) Emitir advertências sobre o não cumprimento, por parte das entidades, das obrigações previstas na presente diretiva;

   b) Emitir instruções vinculativas ou uma ordem que exija que essas entidades corrijam as deficiências detetadas ou as infrações às obrigações previstas na presente diretiva;

   c) Ordenar que essas entidades cessem condutas não conformes com as obrigações previstas na presente diretiva e se abstenham de as repetir;

   d) Ordenar que essas entidades garantam a conformidade das suas medidas de gestão dos riscos ou obrigações de notificação com as obrigações estabelecidas nos artigos 18.º e 20.º de uma forma e num período especificados;

   e) Ordenar que essas entidades informem as pessoas singulares ou coletivas a quem prestam serviços ou atividades que sejam potencialmente afetadas por

uma ciberameaça significativa de quaisquer possíveis medidas de proteção ou corretivas que possam ser tomadas por essas pessoas em resposta a essa ameaça;

f) Ordenar que essas entidades apliquem, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança;

g) Ordenar que essas entidades tornem públicos os aspetos do não cumprimento das suas obrigações estabelecidas na presente diretiva de uma determinada forma;

h) Fazer uma declaração pública que identifique as pessoas singulares e coletivas responsáveis pela violação de uma obrigação prevista na presente diretiva e a natureza dessa violação;

i) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, de acordo com a legislação nacional, de uma coima nos termos do artigo 31.º, em complemento ou em vez das medidas referidas nas alíneas a) a h) do presente número, em função das circunstâncias de cada caso concreto.

5. O artigo 29.º, n.os 6 a 8, aplica-se também às medidas de supervisão e coercivas previstas no presente artigo no respeitante às entidades importantes enumeradas no anexo II.

*Artigo 31.º*

***Condições gerais para a aplicação de coimas a entidades essenciais e importantes***

1. Os Estados-Membros devem assegurar que a aplicação de coimas às entidades essenciais e importantes, nos termos do presente artigo, relativamente a violações das obrigações previstas na presente diretiva é, em cada caso individual, efetiva, proporcionada e dissuasiva.

2. Consoante as circunstâncias de cada caso, as coimas devem ser aplicadas em complemento ou em vez das medidas referidas no artigo 29.º, n.º 4, alíneas a) a i), no artigo 29.º, n.º 5, e no artigo 30.º, n.º 4, alíneas a) a h).

3. Ao decidir sobre a aplicação de uma coima e sobre o seu montante em cada caso individual, devem ser tidos em devida consideração, no mínimo, os elementos previstos no artigo 29.º, n.º 7.

4. Os Estados-Membros devem assegurar que as violações das obrigações previstas nos artigos 18.º ou 20.º são sujeitas, nos termos dos n.os 2 e 3 do presente artigo, a coimas num montante máximo não inferior a 10 000 000 EUR ou 2 % do volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, da empresa a que a entidade essencial ou importante pertence, consoante o montante que for mais elevado.

5. Os Estados-Membros podem prever o poder de aplicar sanções pecuniárias periódicas para obrigar uma entidade essencial ou importante a cessar uma violação em conformidade com uma decisão prévia da autoridade competente.

6. Sem prejuízo dos poderes das autoridades competentes nos termos dos artigos 29.º e 30.º, os Estados-Membros podem adotar regras para determinar se e em que medida podem ser aplicadas coimas às entidades da administração pública na aceção do artigo 4.º, ponto 23, sob reserva das obrigações previstas na presente diretiva.

*Artigo 32.º*

***Infrações que implicam uma violação de dados pessoais***

1. Se as autoridades competentes tiverem indícios de que a infração das obrigações estabelecidas nos artigos 18.º e 20.º por parte de uma entidade essencial ou importante implica uma violação de dados pessoais, na aceção do artigo 4.º, ponto 12, do Regulamento (UE) 2016/679, a qual deve ser notificada nos termos do artigo 33.º do referido regulamento, devem informar as autoridades de controlo competentes nos termos dos artigos 55.º e 56.º do referido regulamento num prazo razoável.

2. Se as autoridades de controlo competentes nos termos dos artigos 55.º e 56.º do Regulamento (UE) 2016/679 decidirem exercer os seus poderes, em conformidade com o artigo 58.º, n.º 2, alínea i), desse regulamento, e aplicar uma coima, as autoridades competentes não podem aplicar uma coima pela mesma infração ao abrigo do artigo 31.º da presente diretiva. As autoridades competentes podem, no entanto, aplicar as medidas coercivas ou exercer os poderes sancionatórios previstos no artigo 29.º, n.º 4, alíneas a) a i), no artigo 29.º, n.º 5, e no artigo 30.º, n.º 4, alíneas a) a h), da presente diretiva.

3. Se a autoridade de controlo competente nos termos do Regulamento (UE) 2016/679 estiver estabelecida num Estado-Membro diferente do da autoridade competente, esta última pode informar a autoridade de controlo estabelecida no seu Estado-Membro.

*Artigo 33.º*

**Sanções**

1. Os Estados-Membros devem estabelecer as regras relativas às sanções aplicáveis em caso de violação das disposições nacionais adotadas nos termos da presente diretiva e tomar todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros devem notificar a Comissão dessas regras e medidas até [dois] anos a contar da data de entrada em vigor da presente diretiva, bem como, imediatamente, de qualquer alteração ulterior das mesmas.

*Artigo 34.º*

**Assistência mútua**

1. Se uma entidade essencial ou importante prestar serviços em mais do que um Estado-Membro, ou tiver o seu estabelecimento principal ou estiver representada num Estado-Membro, mas as suas redes e sistemas de informação estiverem situados noutro ou noutros Estados-Membros, a autoridade competente do Estado-Membro do estabelecimento principal ou de outro estabelecimento ou do representante e as autoridades competentes dos outros Estados-Membros devem cooperar entre si e prestar assistência mútua, na medida do necessário. Essa cooperação deve implicar, no mínimo, que:

a) As autoridades competentes que apliquem medidas de supervisão ou coercivas num Estado-Membro informem e consultem, por intermédio do ponto de contacto único, as autoridades competentes dos outros Estados-Membros em causa sobre as medidas de supervisão e coercivas tomadas e o seu seguimento, nos termos dos artigos 29.º e 30.º;

b) Uma autoridade competente possa solicitar a outra autoridade competente que tome as medidas de supervisão ou coercivas referidas nos artigos 29.º e 30.º;

c) Uma autoridade competente, ao receber um pedido justificado de outra autoridade competente, preste assistência à mesma para que as medidas de supervisão ou coercivas referidas nos artigos 29.º e 30.º possam ser executadas de forma eficaz, eficiente e coerente. Tal assistência mútua pode abranger pedidos de informações e medidas de supervisão, incluindo pedidos para realizar inspeções no local, supervisão remota ou auditorias de segurança específicas. Uma autoridade competente a quem seja dirigido um pedido de assistência não pode recusar esse pedido a menos que, após um intercâmbio com as outras autoridades envolvidas, a ENISA e a Comissão, se determine que a autoridade não tem competência para prestar a assistência solicitada, ou que a assistência solicitada não é proporcionada às funções de supervisão da autoridade competente desempenhadas em conformidade com os artigos 29.º ou 30.º.

2. Quando adequado e de comum acordo, as autoridades competentes de diferentes Estados-Membros podem realizar as ações de supervisão conjuntas referidas nos artigos 29.º e 30.º.

## CAPÍTULO VII

*Disposições transitórias e finais*

*Artigo 35.º*

***Avaliação***

A Comissão avalia periodicamente a aplicação da presente diretiva e apresenta um relatório ao Parlamento Europeu e ao Conselho. O relatório avalia, em particular, a pertinência dos setores, dos subsetores, da dimensão e do tipo de entidades referidas nos anexos I e II para o funcionamento da economia e da sociedade o que diz respeito à cibersegurança. Para esse efeito, e a fim de promover a cooperação estratégica e operacional, a Comissão tem em conta os relatórios do grupo de cooperação e da rede de CSIRT sobre a experiência adquirida a nível estratégico e operacional. O primeiro relatório deve ser apresentado até … [*54 meses após a data de entrada em vigor da presente diretiva*].

*Artigo 36.º*

***Exercício da delegação***

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 18.º, n.º 6, e no artigo 21.º, n.º 2, é conferido à Comissão por um prazo de cinco anos a contar de […].

3. A delegação de poderes referida no artigo 18.º, n.º 6, e no artigo 21.º, n.º 2, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. Produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 18.º, n.º 6, e do artigo 21.º, n.º 2, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

*Artigo 37.º*

***Procedimento de comité***

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

3. Caso o parecer do comité deva ser obtido por procedimento escrito, este é encerrado sem resultados se, no prazo fixado para dar o parecer, o presidente assim o decidir ou um dos seus membros assim o requerer.

*Artigo 38.º*

***Transposição***

1. Os Estados-Membros devem adotar e publicar, até … [*18 meses após a data de entrada em vigor da presente diretiva*], as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Do facto informam imediatamente a Comissão. Os Estados-Membros devem aplicar essas disposições a partir de … [*um dia após a data referida na primeira frase*].

2. As disposições adotadas pelos Estados-Membros devem fazer referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. Os Estados-Membros estabelecem o modo como deve ser feita a referência.

*Artigo 39.º*

***Alteração do Regulamento (UE) n.º 910/2014***

É suprimido o artigo 19.º do Regulamento (UE) n.º 910/2014.

*Artigo 40.º*

***Alteração da Diretiva (UE) 2018/1972***

São suprimidos os artigos 40.º e 41.º da Diretiva (UE) 2018/1972.

*Artigo 41.º*

***Revogação***

A Diretiva (UE) 2016/1148 é revogada com efeitos a partir de … [*data do prazo de transposição da diretiva*].

As remissões para a Diretiva (UE) 2016/1148 devem entender-se como remissões para a presente diretiva e ser lidas de acordo com o quadro de correspondência constante do anexo III.

*Artigo 42.º*

***Entrada em vigor***

A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

*Artigo 43.º*

***Destinatários***

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Bruxelas, em

*Pelo Parlamento Europeu*
*O Presidente*

*Pelo Conselho*
*O Presidente*

**FICHA FINANCEIRA LEGISLATIVA**

# ÍNDICE


1. CONTEXTO DA PROPOSTA/INICIATIVA ..... 2
1.1. Denominação da proposta/iniciativa ..... 2
*1.2.* Domínio(s) de intervenção abrangido(s) *(grupo de programas)* ..... 2
1.3. A proposta/iniciativa refere-se a: ..... 2
1.4. Justificação da proposta/iniciativa ..... 2
1.4.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa ..... 2
1.4.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada. ..... 2
1.4.3. Ensinamentos retirados de experiências anteriores semelhantes ..... 3
1.4.4. Compatibilidade e eventual sinergia com outros instrumentos adequados ..... 3
1.5. Duração e impacto financeiro ..... 4
1.6. Modalidade(s) de gestão prevista(s) ..... 4
2. MEDIDAS DE GESTÃO ..... 6
2.1. Disposições em matéria de acompanhamento e comunicação de informações ..... 6
2.2. Sistema(s) de gestão e de controlo ..... 6
2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos 6
2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar ..... 6
2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento) ..... 6
2.3. Medidas de prevenção de fraudes e irregularidades ..... 6
3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA ..... 7
3.1. Rubrica do quadro financeiro plurianual e nova(s) rubrica(s) orçamental(ais) de despesas proposta(s) ..... 7
3.2. Impacto estimado nas despesas ..... 8
3.2.1. Síntese do impacto estimado nas despesas ..... 8
3.2.2. Síntese do impacto estimado nas dotações de natureza administrativa ..... 11
3.2.3. Participação de terceiros no financiamento ..... 13

3.3. Impacto estimado nas receitas..... 13

## 1. CONTEXTO DA PROPOSTA/INICIATIVA

### 1.1. Denominação da proposta/iniciativa

Proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148

### 1.2. Domínio(s) de intervenção abrangido(s) *(grupo de programas)*

| |
|---|
| Redes de comunicações, conteúdos e tecnologias |

### 1.3. A proposta/iniciativa refere-se a:

☐ **uma nova ação**

☐ **uma nova ação na sequência de um projeto-piloto/ação preparatória**[40]

☒ **uma prorrogação de uma ação existente**

☐ **uma fusão ou reorientação de uma ou mais ações para outra/uma nova ação**

### 1.4. Justificação da proposta/iniciativa

*1.4.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa*

| |
|---|
| A revisão visa aumentar o nível de ciber-resiliência de um conjunto abrangente de empresas que operam na União Europeia em todos os setores importantes, reduzir as diferenças em termos de resiliência no mercado interno nos setores já abrangidos pela diretiva, e melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta. |

*1.4.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.*

| |
|---|
| A ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de medidas nacionais ou regionais estanques. A Diretiva SRI surgiu para colmatar esta lacuna, estabelecendo um quadro para a segurança das redes e dos sistemas de informação a nível nacional e da União. No entanto, a primeira avaliação periódica da Diretiva SRI revelou várias deficiências intrínsecas, que acabaram por levar a disparidades consideráveis entre os Estados-Membros em termos de capacidades, planeamento e nível de proteção, e que, ao mesmo tempo, afetam a equidade das condições de concorrência para empresas similares no mercado interno.<br><br>A intervenção da UE, indo além das atuais medidas previstas na Diretiva SRI, justifica-se principalmente: i) pelo carácter transfronteiriço do problema; ii) pelo potencial da ação da UE para melhorar e facilitar a eficácia das políticas nacionais; iii) pelo contributo de ações concertadas e colaborativas de política em matéria de SRI para uma proteção eficaz dos dados e da privacidade. |

[40] Como referido no artigo 58.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

Assim, os objetivos enumerados podem ser mais facilmente alcançados por uma ação a nível da UE do que pelos Estados-Membros agindo isoladamente.

*1.4.3. Ensinamentos retirados de experiências anteriores semelhantes*

A Diretiva SRI é o primeiro instrumento horizontal do mercado interno destinado a melhorar a resiliência das redes e dos sistemas na União contra os riscos de cibersegurança, tendo contribuído, em grande medida, para aumentar o nível comum de cibersegurança entre os Estados-Membros. No entanto, a avaliação do funcionamento e da aplicação da diretiva revelou várias deficiências que, juntamente com a crescente digitalização e a necessidade de uma resposta mais atualizada, devem ser abordadas por via de um ato jurídico revisto.

*1.4.4. Compatibilidade e eventual sinergia com outros instrumentos adequados*

A nova proposta é inteiramente compatível e coerente com outras iniciativas relacionadas, como a proposta de regulamento relativo à resiliência operacional digital do setor financeiro («DORA») e a proposta de diretiva relativa à resiliência de operadores críticos de serviços essenciais. É também coerente com o Código Europeu das Comunicações Eletrónicas, o Regulamento Geral sobre a Proteção de Dados e o Regulamento eIDAS.

A proposta é uma parte essencial da Estratégia para a União da Segurança.

## 1.5. Duração e impacto financeiro

☐ **duração limitada**

– ☐ em vigor entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA para as dotações de autorização e entre AAAA a AAAA para as dotações de pagamento.

☒ **duração ilimitada**

– Aplicação com um período de arranque entre 2022 e 2025

– seguido de um período de aplicação a um ritmo de cruzeiro.

## 1.6. Modalidade(s) de gestão prevista(s)[41]

**Gestão direta** pela Comissão

– ☒ pelos seus serviços, incluindo o pessoal nas delegações da União;

– ☐ pelas agências de execução

☐ **Gestão partilhada** com os Estados-Membros

☐ **Gestão indireta**, confiando tarefas de execução orçamental:

– ☐ a países terceiros ou a organismos por estes designados;

– ☐ a organizações internacionais e respetivas agências (a especificar);

– ☐ ao BEI e ao Fundo Europeu de Investimento;

– X☐ aos organismos referidos nos artigos 70.º e 71.º do Regulamento Financeiro;

– ☐ a organismos de direito público;

– ☐ a organismos regidos pelo direito privado com uma missão de serviço público, na medida em que prestem garantias financeiras adequadas;

– ☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

– ☐ a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

– *Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».*

Observações

A Agência da União Europeia para a Cibersegurança (ENISA), à qual foi conferido um novo mandato permanente pelo Regulamento Cibersegurança, ajudaria os Estados-Membros e a Comissão na aplicação da Diretiva SRI revista.

Como resultado da Diretiva SRI revista, a partir de 2022-2023, a ENISA terá domínios de ação adicionais. Embora estes domínios de ação estejam abrangidos pelas atribuições gerais da ENISA de acordo com o seu mandato, significarão numa carga de trabalho adicional para a agência. Mais precisamente, além dos seus atuais domínios de ação, nos termos da proposta

[41] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

da Comissão de uma Diretiva SRI revista, a ENISA deverá também incorporar especificamente no seu programa de trabalho, nomeadamente, as seguintes ações: i) criar e manter um registo europeu de vulnerabilidades (artigo 6.º, n.º 2, da proposta); ii) assegurar os serviços de secretariado da Rede Europeia de Organizações de Coordenação de Cibercrises (CyCLONe) (artigo 14.º da proposta) e elaborar um relatório anual sobre o estado da cibersegurança na UE (artigo 15.º da proposta); iii) apoiar a organização de análises pelos pares entre Estados-Membros (artigo 16.º da proposta); iv) recolher dados agregados sobre incidentes dos Estados-Membros e emitir orientações técnicas (artigo 20.º, n.º 9, da proposta); v) criar e manter um registo de entidades que prestam serviços transfronteiriços (artigo 25.º da proposta).

Por conseguinte, será apresentado um pedido de 5 ETI suplementares a partir de 2022, com o orçamento correspondente de cerca de 0,61 milhões de EUR por ano, para cobrir estes novos lugares (ver ficha financeira separada para as agências).

## 2. MEDIDAS DE GESTÃO

### 2.1. Disposições em matéria de acompanhamento e comunicação de informações

*Especificar a periodicidade e as condições.*

| |
|---|
| A Comissão avaliará periodicamente a aplicação da diretiva e apresentará um relatório ao Parlamento Europeu e ao Conselho, a primeira vez três anos após a sua entrada em vigor.<br><br>A Comissão avaliará igualmente a transposição correta da diretiva pelos Estados-Membros. |

### 2.2. Sistema(s) de gestão e de controlo

*2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos*

| |
|---|
| A unidade da DG CNECT responsável pelo domínio de intervenção fará a gestão da aplicação da diretiva. |

*2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar*

| |
|---|
| Risco muito baixo, uma vez que o ecossistema da Diretiva SRI já está estabelecido. |

*2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)*

| |
|---|
| Não aplicável. Utilização exclusiva do orçamento administrativo («dotação global»). |

### 2.3. Medidas de prevenção de fraudes e irregularidades

*Especificar as medidas de prevenção e de proteção existentes ou previstas, como, por exemplo, da estratégia antifraude*

| |
|---|
| Não aplicável. Utilização exclusiva do orçamento administrativo («dotação global»). |

## 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

### 3.1. Rubrica do quadro financeiro plurianual e nova(s) rubrica(s) orçamental(ais) de despesas proposta(s)

| Rubrica do quadro financeiro plurianual | Rubrica orçamental | Tipo de despesa | Participação | | | |
|---|---|---|---|---|---|---|
| | Número [Rubrica…7……...……] | DD/DND[42] | dos países da EFTA[43] | dos países candidatos[44] | de países terceiros | na aceção do artigo [21.º, n.º 2, alínea b)] do Regulamento Financeiro |
| | 20 02 06 despesas de gestão<br><br>20 02 06 | DND | NÃO | NÃO | NÃO | NÃO |

[42] DD = dotações diferenciadas/DND = dotações não diferenciadas.

[43] EFTA: Associação Europeia de Comércio Livre.

[44] Países candidatos e, se aplicável, países candidatos potenciais dos Balcãs Ocidentais.

## 3.2. Impacto estimado nas despesas

### *3.2.1. Síntese do impacto estimado nas despesas*

Em milhões de EUR (três casas decimais)

| **Rubrica do quadro financeiro plurianual** | **<…>** | [Rubrica……...……] |
|---|---|---|

| | | | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | ***Após 2027*** | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Dotações operacionais (repartidas de acordo com as rubricas orçamentais referidas no ponto 3.1) | Autorizações | (1) | | | | | | | | | |
| | Pagamentos | (2) | | | | | | | | | |
| Dotações de natureza administrativa financiadas a partir da dotação do programa[45] | Autorizações = Pagamentos | (3) | | | | | | | | | |
| **TOTAL das dotações para o enquadramento financeiro do programa** | Autorizações | =1+3 | | | | | | | | | |
| | Pagamentos | =2+3 | | | | | | | | | |

| **Rubrica do quadro financeiro plurianual** | 7 | «Despesas administrativas»<br>Reuniões: as reuniões plenárias do grupo de cooperação SRI realizam-se, geralmente, 4 vezes por ano. A Comissão cobre os custos relacionados com a restauração e as despesas de viagem dos representantes de 27 Estados-Membros (um representante por Estado-Membro). Os custos de uma reunião podem chegar aos 15 000 EUR.<br>Deslocações em serviço: as deslocações em serviço estão relacionadas com o acompanhamento da aplicação da Diretiva SRI. Exemplo: no espaço de um ano (de maio de 2019 a julho de 2020) deveríamos ter organizado visitas aos países no âmbito |
|---|---|---|

[45] Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

| | | |
|---|---|---|
| | | da SRI e visitado os 27 Estados-Membros para discutir a aplicação da Diretiva SRI em toda a UE. |

Esta secção deve ser preenchida com «dados orçamentais de natureza administrativa» a inserir em primeiro lugar no Anexo da ficha financeira legislativa, que é carregado no DECIDE para efeitos das consultas interserviços.

Em milhões de EUR (três casas decimais)

| | | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | *Após 2027* | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| Recursos humanos | | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | **1,14** | | **7,98** |
| Outras despesas administrativas | | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | | **0,63** |
| **TOTAL das dotações no âmbito da RUBRICA 7 do quadro financeiro plurianual** | (Total das autorizações = total dos pagamentos) | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | | **8,61** |

Em milhões de EUR (três casas decimais)

| | | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | *Após 2027* | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações no âmbito das RUBRICAS** do quadro financeiro plurianual | Autorizações | | | | | | | | | |
| | Pagamentos | | | | | | | | | |

*3.2.2. Síntese do impacto estimado nas dotações de natureza administrativa*

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– ☐X A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

| **Anos** | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| **RUBRICA 7 do quadro financeiro plurianual** | | | | | | | | |
| Recursos humanos | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | **1,14** | **7,98** |
| Outras despesas administrativas | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | **0,09** | **0,63** |
| **Subtotal RUBRICA 7 do quadro financeiro plurianual** | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | **1,23** | **8,61** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Com exclusão da RUBRICA 7[46] of the multiannual financial framework** | | | | | | | | |
| Recursos humanos | | | | | | | | |
| Outras despesas de natureza administrativa | | | | | | | | |
| **Subtotal com exclusão da RUBRICA 7 do quadro financeiro plurianual** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **8,61** |

As dotações relativas aos recursos humanos e outras despesas administrativas necessárias serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas na DG e, se necessário, pelas eventuais dotações adicionais que sejam concedidas à DG gestora no âmbito do processo de afetação anual e atendendo às restrições orçamentais.

[46] Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

3.2.2.1. Necessidades estimadas de recursos humanos

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos.

– X☐ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

*As estimativas devem ser expressas em termos de equivalente a tempo inteiro*

| **Anos** | | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** |
|---|---|---|---|---|---|---|---|---|
| **• Lugares do quadro do pessoal (funcionários e agentes temporários)** | | | | | | | | |
| Sede e gabinetes de representação da Comissão | | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| Delegações | | | | | | | | |
| Investigação | | | | | | | | |
| **• Pessoal externo (em equivalente a tempo inteiro: ETI) — AC, AL, PND, TT e JPD** [47] Rubrica 7 | | | | | | | | |
| Financiado a partir da RUBRICA 7 do quadro financeiro plurianual | — na sede | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| | — nas delegações | | | | | | | |
| Financiado a partir do enquadramento financeiro do programa [48] | — na sede | | | | | | | |
| | — nas delegações | | | | | | | |
| Investigação | | | | | | | | |
| Outros (especificar) | | | | | | | | |
| **TOTAL** | | **9** | **9** | **9** | **9** | **9** | **9** | **9** |

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

| | |
|---|---|
| Funcionários e agentes temporários | • Elaboração de atos delegados de acordo com o artigo 18.º, n.º 6, o artigo 21.º, n.º 2, e o artigo 36.º;<br>• Elaboração de atos de execução de acordo com o artigo 12.º, n.º 8, o artigo 18.º, n.º 5, e o artigo 20.º, n.º 11;<br>• Prestação dos serviços de secretariado do grupo de cooperação SRI;<br>• Organização das reuniões plenárias e das vertentes de trabalho do grupo de cooperação SRI;<br>• Coordenação do trabalho dos Estados-Membros relativamente a vários documentos (orientações, conjuntos de instrumentos, etc.);<br>• Coordenação com outros serviços da Comissão, a ENISA e as autoridades nacionais com vista à aplicação da Diretiva SRI;<br>• Análise de boas práticas e métodos nacionais relacionados com a aplicação da Diretiva SRI. |
| Pessoal externo | Apoiar todas as tarefas acima mencionadas, conforme for necessário |

[47] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

[48] Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

*3.2.3. Participação de terceiros no financiamento*

A proposta/iniciativa:

– X☐ não prevê o cofinanciamento por terceiros

– ☐ prevê o cofinanciamento por terceiros a seguir estimado:

Dotações em milhões de EUR (três casas decimais)

| **Anos** | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Especificar o organismo de cofinanciamento | | | | | | | | |
| TOTAL das dotações cofinanciadas | | | | | | | | |

## 3.3. Impacto estimado nas receitas

– ☐X A proposta/iniciativa não tem impacto financeiro nas receitas.

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

☐ nos recursos próprios

☐ noutras receitas

indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

| Rubrica orçamental das receitas: | Impacto da proposta/iniciativa[49] | | | | | | |
|---|---|---|---|---|---|---|---|
| | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** |
| Artigo ……. | | | | | | | |

Relativamente às receitas afetadas, especificar a(s) rubrica(s) orçamental(ais) de despesas envolvida(s).

Outras observações (p. ex., método/fórmula utilizado/a para o cálculo do impacto sobre as receitas ou qualquer outra informação).

[49] No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.

# ANEXO
# da FICHA FINANCEIRA LEGISLATIVA

Denominação da proposta/iniciativa:

Proposta de diretiva de revisão da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

……
……

**1. NÚMERO e CUSTO dos RECURSOS HUMANOS CONSIDERADOS NECESSÁRIOS**

**2. CUSTO de OUTRAS DESPESAS DE NATUREZA ADMINISTRATIVA**

**3. MÉTODOS de CÁLCULO UTILIZADOS para ESTIMAR os CUSTOS**

**3.1 Recursos humanos**

**3.2 Outras despesas administrativas**

*Este anexo, **a preencher por cada DG/serviço que participa na proposta/iniciativa**, deve acompanhar a ficha financeira legislativa aquando do lançamento da consulta interserviços.*

*Os quadros com dados são utilizados como fonte nos quadros incluídos na ficha financeira legislativa. São exclusivamente para uso interno na Comissão.*

1. Custo dos recursos humanos considerados necessários

☐ A proposta/iniciativa não acarreta a utilização de recursos humanos

X☐ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

| **RUBRICA 7** do quadro financeiro plurianual | | **2021** | | **2022** | | **2023** | | **2024** | | **2025** | | **2026** | | **2027** | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações |
| **• Lugares do quadro do pessoal (funcionários e agentes temporários)** | | | | | | | | | | | | | | | | | |
| Sede e gabinetes de representação da Comissão | AD | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 42 | 6,3 |
| | AST | | | | | | | | | | | | | | | | |
| Nas delegações da União | AD | | | | | | | | | | | | | | | | |
| | AST | | | | | | | | | | | | | | | | |
| **• Pessoal externo[50] 0,24** | | | | | | | | | | | | | | | | | |
| Dotação global | AC | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 21 | 1,68 |
| | PND | | | | | | | | | | | | | | | | |
| | TT | | | | | | | | | | | | | | | | |
| Nas delegações da União | AC | | | | | | | | | | | | | | | | |
| | AL | | | | | | | | | | | | | | | | |
| | PND | | | | | | | | | | | | | | | | |

[50] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | TT | | | | | | | | | | | | | | | | |
| | JPD | | | | | | | | | | | | | | | | |
| Outras rubricas orçamentais (*especificar*) | | | | | | | | | | | | | | | | | |
| **Subtotal – RUBRICA 7** do quadro financeiro plurianual | | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 63 | 7,98 |

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

| Com exclusão da RUBRICA 7 do quadro financeiro plurianual | | 2021 | | 2022 | | 2023 | | 2024 | | 2025 | | 2025 | | 2025 | | TOTAL | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações | ETI | Dotações |
| **• Lugares do quadro do pessoal (funcionários e agentes temporários)** | | | | | | | | | | | | | | | | | |
| Investigação | AD | | | | | | | | | | | | | | | | |
| | AST | | | | | | | | | | | | | | | | |
| **• Pessoal externo[51]** | | | | | | | | | | | | | | | | | |
| Pessoal externo previsto nas dotações operacionais (antigas rubricas «BA»). | — na sede — AC | | | | | | | | | | | | | | | | |
| | — na sede — PND | | | | | | | | | | | | | | | | |
| | — na sede — TT | | | | | | | | | | | | | | | | |
| | — nas delegações da União — AC | | | | | | | | | | | | | | | | |
| | — nas delegações da União — AL | | | | | | | | | | | | | | | | |
| | — nas delegações da União — PND | | | | | | | | | | | | | | | | |
| | — nas delegações da União — TT | | | | | | | | | | | | | | | | |
| | — nas delegações da União — JPD | | | | | | | | | | | | | | | | |
| Investigação | AC | | | | | | | | | | | | | | | | |
| | PND | | | | | | | | | | | | | | | | |
| | TT | | | | | | | | | | | | | | | | |
| Outras rubricas orçamentais | | | | | | | | | | | | | | | | | |

[51] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (*especificar*) | | | | | | | | | | | | | | | | | |
| **Subtotal – Com exclusão da RUBRICA 7**<br>do quadro financeiro plurianual | | | | | | | | | | | | | | | | | |

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

*Impacto estimado nos recursos humanos da ENISA*

A Agência da União Europeia para a Cibersegurança (ENISA), à qual foi conferido um novo mandato permanente pelo Regulamento Cibersegurança, ajudaria os Estados-Membros e a Comissão na aplicação da Diretiva SRI revista.

Como resultado da Diretiva SRI revista, a partir de 2022-2023, a ENISA terá domínios de ação adicionais. Embora estes domínios de ação estejam abrangidos pelas atribuições gerais da ENISA de acordo com o seu mandato, significarão numa carga de trabalho adicional para a agência. Mais precisamente, além dos seus atuais domínios de ação, nos termos da proposta da Comissão de uma Diretiva SRI revista, a ENISA deverá também incorporar especificamente no seu programa de trabalho, nomeadamente, as seguintes ações: i) criar e manter um registo europeu de vulnerabilidades (artigo 6.º, n.º 2, da proposta); ii) assegurar os serviços de secretariado da Rede Europeia de Organizações de Coordenação de Cibercrises (CyCLONe) (artigo 14.º da proposta) e elaborar um relatório anual sobre o estado da cibersegurança na UE (artigo 15.º da proposta); iii) apoiar a organização de análises pelos pares entre Estados-Membros (artigo 16.º da proposta); iv) recolher dados agregados sobre incidentes dos Estados-Membros e emitir orientações técnicas (artigo 20.º, n.º 9, da proposta); v) criar e manter um registo de entidades que prestam serviços transfronteiriços (artigo 25.º da proposta).

Por conseguinte, será apresentado um pedido de 5 ETI suplementares a partir de 2022, com o orçamento correspondente de cerca de 0,61 milhões de EUR por ano, para cobrir estes novos lugares (ver ficha financeira separada para as agências).

Por conseguinte, será apresentado um pedido de 5 ETI suplementares a partir de 2022, com o orçamento correspondente para cobrir estes novos lugares.

☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

☐X A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

| | Ano **N**[52] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | **TOTAL** |
|---|---|---|---|---|---|---|

[52] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Agentes temporários (graus AD) | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | | **2,7** |
| Agentes temporários (graus AST) | | | | | | | | |
| Agentes contratuais | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | | |
| Peritos nacionais destacados | | | | | | | | **0,96** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | | **3,66** |

Necessidades de pessoal (ETI):

| | Ano **N**[53] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agentes temporários (graus AD) | 3 | 3 | 3 | 3 | 3 | 3 | | **18** |
| Agentes temporários (graus AST) | | | | | | | | |
| Agentes contratuais | 2 | 2 | 2 | 2 | 2 | 2 | | **12** |

[53] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Peritos nacionais destacados | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **5** | **5** | **5** | **5** | **5** | **5** | | **30** |

2. Custo de outras despesas de natureza administrativa

☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

X☐ A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

*Em milhões de EUR (três casas decimais)*

| **RUBRICA 7** do quadro financeiro plurianual | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **Total** |
|---|---|---|---|---|---|---|---|---|
| **Na sede:** | | | | | | | | |
| Despesas de deslocações em serviço e de representação | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | **0,21** |
| Despesas relativas a conferências e reuniões | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | **0,42** |
| Comités[54] | | | | | | | | |
| Estudos e consultas | | | | | | | | |

[54] Especificar o tipo de comité e o grupo a que este pertence.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Sistemas de informação e gestão | | | | | | | | |
| Equipamento e serviços de TIC[55] | | | | | | | | |
| Outras rubricas orçamentais (*especificar se for caso disso*) | | | | | | | | |
| **Nas delegações da União** | | | | | | | | |
| Despesas de deslocações em serviço, conferências e representação | | | | | | | | |
| Formação do pessoal | | | | | | | | |
| Aquisição, arrendamento e despesas conexas | | | | | | | | |
| Equipamento, mobiliário, fornecimentos e serviços | | | | | | | | |
| **Subtotal RUBRICA 7**<br>do quadro financeiro plurianual | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | **0,63** |

[55] TIC: Tecnologias da informação e comunicação: é necessário consultar a DIGIT.

*Em milhões de EUR (três casas decimais)*

| **Com exclusão da RUBRICA 7** do quadro financeiro plurianual | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **Total** |
|---|---|---|---|---|---|---|---|---|
| Despesas de assistência técnica e administrativa (não incluindo o pessoal externo) a partir de dotações operacionais (antigas rubricas «BA») | | | | | | | | |
| — na sede | | | | | | | | |
| — nas delegações da União | | | | | | | | |
| Outras despesas de gestão no domínio da investigação | | | | | | | | |
| Outras rubricas orçamentais (*especificar se for caso disso*) | | | | | | | | |
| **Subtotal – Com exclusão da RUBRICA 7** do quadro financeiro plurianual | | | | | | | | |

| **TOTAL RUBRICA 7 e com exclusão da RUBRICA 7** do quadro financeiro plurianual | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | **8,61** |
|---|---|---|---|---|---|---|---|---|

As dotações administrativas necessárias serão cobertas por dotações já afetadas à gestão da ação e/ou reafetadas, complementadas se necessário por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

3. Métodos de cálculo utilizados para estimar os custos

3.1 Recursos humanos

*Esta parte define o método de cálculo utilizado para estimar os recursos humanos considerados necessários [carga de trabalho prevista, incluindo funções específicas (perfis do Sysper 2), categorias de pessoal e custos médios correspondentes]*

| **RUBRICA 7** do quadro financeiro plurianual |
|---|
| N.B.: Os custos médios por categoria de pessoal na sede estão disponíveis na BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx |
| • Funcionários e agentes temporários<br>6 funcionários ETI (custo médio 0,150) = 0,9 por ano<br>- Elaboração de atos delegados de acordo com o artigo 18.º, n.º 6, o artigo 21.º, n.º 2, e o artigo 36.º;<br>- Elaboração de atos de execução de acordo com o artigo 12.º, n.º 8, o artigo 18.º, n.º 5, e o artigo 20.º, n.º 11;<br>- Prestação dos serviços de secretariado do grupo de cooperação SRI;<br>- Organização das reuniões plenárias e das vertentes de trabalho do grupo de cooperação SRI;<br>- Coordenação do trabalho dos Estados-Membros relativamente a vários documentos (orientações, conjuntos de instrumentos, etc.);<br>- Coordenação com outros serviços da Comissão, a ENISA e as autoridades nacionais com vista à aplicação da Diretiva SRI;<br>- Análise de boas práticas e métodos nacionais relacionados com a aplicação da Diretiva SRI. |
| • Pessoal externo<br>3 AC (custo médio 0,08) = 0,24 por ano<br>- Apoiar todas as tarefas acima mencionadas, conforme for necessário |

| **Com exclusão da RUBRICA 7** do quadro financeiro plurianual |
|---|
| • Apenas os postos financiados pelo orçamento dedicado à investigação |
| • Pessoal externo |

3.2 Outras despesas administrativas

*Especificar detalhadamente os métodos de cálculo utilizados para cada rubrica orçamental,*

*em especial as estimativas de base (nomeadamente, número de reuniões por ano, custos médios, etc.)*

**RUBRICA 7** do quadro financeiro plurianual

Reuniões: as reuniões plenárias do grupo de cooperação SRI realizam-se, geralmente, 4 vezes por ano. A Comissão cobre os custos relacionados com a restauração e as despesas de viagem dos representantes de 27 Estados-Membros (um representante por Estado-Membro). Os custos de uma reunião podem chegar aos 15 000 EUR, o que corresponde a 60 000 EUR por ano.

Deslocações em serviço: as deslocações em serviço estão relacionadas com o acompanhamento da aplicação da Diretiva SRI. Exemplo: no espaço de um ano (de maio de 2019 a julho de 2020) deveríamos ter organizado visitas aos países no âmbito da SRI e visitado os 27 Estados-Membros para discutir

a aplicação da Diretiva SRI em toda a UE.

**Com exclusão da RUBRICA 7** do quadro financeiro plurianual

**ANEXO 7**

**da**
**DECISÃO DA COMISSÃO**

**que estabelece as regras internas sobre a execução do orçamento geral da União Europeia (secção «Comissão Europeia») à atenção dos serviços da Comissão**

# FICHA FINANCEIRA LEGISLATIVA «AGÊNCIAS»

**A presente ficha financeira legislativa abrange o pedido de aumento do pessoal da ENISA em 5 ETI a partir de 2022 para realizar atividades suplementares ligadas à aplicação da Diretiva SRI. Tais atividades já estão abrangidas pelo mandato da ENISA.**

**FICHA FINANCEIRA LEGISLATIVA**

# Índice


1. CONTEXTO DA PROPOSTA/INICIATIVA ..... 15
1.1. Denominação da proposta/iniciativa ..... 15
1.2. Domínio(s) de intervenção abrangido(s) ..... 15
1.3. A proposta refere-se a: ..... 15
1.4. Objetivo(s) ..... 15
1.4.1. Objetivos gerais ..... 15
1.4.2. Objetivo(s) específico(s) ..... 15
1.4.3. Resultados e impacto esperados ..... 17
1.4.4. Indicadores de resultados ..... 18
1.5. Justificação da proposta/iniciativa ..... 18
1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa ..... 18
1.5.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada. ..... 19
1.5.3. Ensinamentos retirados de experiências anteriores semelhantes ..... 19
1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados ..... 19
1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação ..... 19
1.6. Duração e impacto financeiro da proposta/iniciativa ..... 21
1.7. Modalidade(s) de gestão prevista(s) ..... 21
2. MEDIDAS DE GESTÃO ..... 23
2.1. Disposições em matéria de acompanhamento e comunicação de informações ..... 23
2.2. Sistema(s) de gestão e de controlo ..... 23
2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos ..... 23
2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar ..... 23
2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento) ..... 23
2.3. Medidas de prevenção de fraudes e irregularidades ..... 24

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA ..... 24
3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s) ..... 24
3.2. Impacto estimado nas despesas ..... 26
3.2.1. Síntese do impacto estimado nas despesas ..... 26
3.2.2. Impacto estimado nas dotações do(a) [organismo] ..... 28
3.2.3. Impacto estimado nos recursos humanos da ENISA ..... 29
3.2.4. Compatibilidade com o atual quadro financeiro plurianual ..... 32
3.2.5. Participação de terceiros no financiamento ..... 32
3.3. Impacto estimado nas receitas ..... 33

## 1. CONTEXTO DA PROPOSTA/INICIATIVA

### 1.1. Denominação da proposta/iniciativa

Proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148

### 1.2. Domínio(s) de intervenção abrangido(s)

Redes de comunicações, conteúdos e tecnologias

### 1.3. A proposta refere-se a:

☐ **uma nova ação**

☐ **uma nova ação na sequência de um projeto-piloto/ação preparatória**[56]

☒ **uma prorrogação de uma ação existente**

☐ **uma fusão de uma ou mais ações noutra/numa nova ação**

### 1.4. Objetivo(s)

*1.4.1. Objetivos gerais*

A revisão visa aumentar o nível de ciber-resiliência de um conjunto abrangente de empresas que operam na União Europeia em todos os setores importantes, reduzir as diferenças em termos de resiliência no mercado interno nos setores já abrangidos pela diretiva, e melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta.

*1.4.2. Objetivo(s) específico(s)*

A fim de resolver o problema do baixo nível de ciber-resiliência das empresas que operam na União Europeia, o objetivo específico consiste em assegurar que as entidades de todos os setores que dependem de redes e sistemas de informação, e que prestam serviços fundamentais à economia e à sociedade no seu conjunto, sejam obrigadas a tomar medidas de cibersegurança e a notificar incidentes com vista a aumentar o nível global de ciber-resiliência em todo o mercado interno.

A fim de resolver o problema das diferenças em termos de resiliência entre Estados-Membros e setores, o objetivo específico consiste em assegurar que todas as entidades ativas em setores abrangidos pelo quadro jurídico para a SRI, que sejam similares em dimensão e tenham um papel comparável, estejam sujeitas ao mesmo regime regulamentar (estejam ou não abrangidas pelo âmbito de aplicação), independentemente da jurisdição a que pertencem na UE.

A fim de garantir que todas as entidades ativas nos setores abrangidos pelo quadro jurídico para a SRI tenham as mesmas obrigações com base no conceito de gestão dos riscos, quando se trata de medidas de segurança, e tenham de comunicar todos os incidentes com base num conjunto uniforme de critérios, os objetivos específicos consistem em assegurar que as autoridades competentes façam cumprir as regras estabelecidas pelo instrumento jurídico de forma mais eficaz graças a uma harmonização das medidas de supervisão e coercivas, e em assegurar que, entre os Estados-Membros, haja um nível comparável de recursos atribuídos às

[56] Como referido no artigo 58.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

autoridades competentes, que lhes permitam desempenhar as funções essenciais estabelecidas pelo quadro para a SRI.

A fim de resolver o problema do baixo nível de conhecimento situacional comum e da inexistência de mecanismos de resposta conjunta a situações de crise, o objetivo específico consiste em assegurar o intercâmbio de informações essenciais entre os Estados-Membros, introduzindo obrigações claras para as autoridades competentes em matéria de partilha de informações e cooperação em caso de ciberameaças e incidentes, e desenvolvendo uma capacidade de resposta operacional conjunta da União a situações de crise.

### *1.4.3. Resultados e impacto esperados*

*Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada*

Prevê-se que a proposta traga benefícios significativos: as estimativas indicam que pode levar a uma redução no custo dos incidentes de cibersegurança de 11 300 milhões de EUR. O âmbito setorial seria consideravelmente alargado ao abrigo do quadro para a SRI e, além dos benefícios acima referidos, os encargos que poderão resultar dos requisitos em matéria de SRI, nomeadamente do ponto de vista da supervisão, também seriam equilibrados, tanto para as novas entidades a abranger como para as autoridades competentes, uma vez que o novo quadro para a SRI estabeleceria uma abordagem de dois níveis, centrada em entidades grandes e fundamentais, e uma diferenciação do regime de supervisão que permite apenas a supervisão *ex post* para um grande número dessas entidades, nomeadamente as consideradas «importantes», mas não «essenciais».

No geral, a proposta levaria a sinergias e soluções de compromisso eficientes, tendo o maior potencial, de entre todas as opções políticas analisadas, para assegurar um nível de ciber-resiliência acrescido e coerente das entidades fundamentais em toda a União, que acabaria por originar uma poupança de custos tanto para as empresas como para a sociedade.

Implicaria também determinados custos em matéria de conformidade e de execução coerciva para as autoridades competentes dos Estados-Membros (estima-se um aumento global de cerca de 20 % a 30 % dos recursos). No entanto, o novo quadro também traria benefícios substanciais decorrentes de uma melhor panorâmica das principais empresas e de uma interação acrescida com as mesmas, de um reforço da cooperação operacional transfronteiriça, e de mecanismos de assistência mútua e de análise pelos pares. Tal levaria a um reforço global das capacidades de cibersegurança em todos os Estados-Membros.

No respeitante às empresas que ficariam abrangidas pelo âmbito de aplicação do quadro para a SRI, estima-se que precisariam de um aumento máximo de 22 % das suas atuais despesas com segurança das TIC durante os primeiros anos após a sua introdução (que seria de 12 % para as empresas já abrangidas pelo âmbito de aplicação da atual Diretiva SRI). No entanto, este aumento médio das despesas com a segurança das TIC levaria a um benefício proporcional de tais investimentos, nomeadamente devido a uma redução considerável do custo dos incidentes de cibersegurança (estimada em 118 mil milhões de EUR em dez anos).

As pequenas e microempresas ficariam isentas do âmbito de aplicação do quadro para a SRI. No caso das médias empresas, verificar-se-ia provavelmente um aumento do nível das despesas com a segurança das TIC nos primeiros anos após a introdução do novo quadro para a SRI. Ao mesmo tempo, o reforço dos requisitos de segurança para estas entidades fomentaria também as suas capacidades de cibersegurança e ajudaria a melhorar a sua gestão dos riscos associados às TIC.

Haveria um impacto nos orçamentos e nas administrações públicas nacionais: seria de esperar um aumento estimado de aproximadamente 20 % a 30 % dos recursos a curto e médio prazo.

Não são esperados outros impactos negativos significativos. Espera-se que a proposta conduza a capacidades mais sólidas em matéria de cibersegurança e, consequentemente, tenha um impacto atenuante mais substancial no número e na gravidade dos incidentes, incluindo das violações de dados. É também provável que tenha um impacto positivo na garantia de condições de concorrência equitativas em todos os Estados-Membros para as entidades abrangidas pelo âmbito da Diretiva SRI, e que reduza as assimetrias em termos de informações sobre cibersegurança.

*1.4.4. Indicadores de resultados*

*Especificar os indicadores que permitem acompanhar os progressos e os resultados.*

A avaliação dos indicadores será realizada pela Comissão, com o apoio da ENISA e do grupo de cooperação, e terá início três anos após a entrada em vigor do novo ato jurídico em matéria de SRI. Alguns dos indicadores de acompanhamento com base nos quais o sucesso da revisão da Diretiva SRI seria avaliado são os seguintes:

- Melhoria do tratamento de incidentes: ao tomarem medidas de cibersegurança, as empresas estão não só a melhorar a sua capacidade de evitar por completo determinados incidentes, mas também a sua capacidade de resposta aos mesmos. As medidas de sucesso são, portanto: i) a redução do tempo médio necessário para detetar um incidente; ii) o tempo médio que as organizações demoram a recuperar de um incidente; iii) o custo médio dos danos causados por um incidente.

- Maior consciência dos riscos de cibersegurança por parte dos quadros superiores das empresas: ao exigir que as empresas tomem medidas, uma Diretiva SRI revista contribuiria para aumentar a sensibilização dos quadros superiores das empresas para os riscos relacionados com a cibersegurança. Tal pode ser medido, estudando até que ponto as empresas abrangidas pelo âmbito da Diretiva SRI dão prioridade à cibersegurança nas suas políticas e processos internos, conforme evidenciado por documentação interna, programas de formação pertinentes e atividades de sensibilização para os trabalhadores, bem como a investimentos em TIC relacionados com a segurança. Os quadros superiores de todas as entidades essenciais e importantes devem estar igualmente conscientes das regras estabelecidas pela Diretiva SRI.

- Nivelamento de despesas setoriais específicas: as despesas com a segurança das TIC variam consideravelmente entre setores na UE. Ao exigir que as empresas de mais setores tomem medidas, os desvios em relação à média das despesas setoriais específicas com a segurança das TIC, enquanto percentagem das despesas globais com TIC, devem diminuir entre setores e entre Estados-Membros.

- Autoridades competentes mais fortes e reforço da cooperação: uma Diretiva SRI revista conferiria potencialmente funções adicionais às autoridades competentes. Tal teria um impacto mensurável nos recursos financeiros e humanos consagrados às agências de cibersegurança a nível nacional, e deveria igualmente ter um impacto positivo na capacidade das autoridades competentes de cooperarem de forma proativa e, por conseguinte, aumentarem o número de casos em que cooperam com o objetivo de lidarem com incidentes transfronteiriços ou realizarem atividades de supervisão conjuntas.

- Maior partilha de informações: a Diretiva SRI revista também melhoraria a partilha de informações entre empresas e com as autoridades competentes. Um dos objetivos da revisão poderia ser aumentar o número de entidades que participam nos vários mecanismos de partilha de informações.

**1.5. Justificação da proposta/iniciativa**

*1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa*

A proposta visa aumentar o nível de ciber-resiliência de um conjunto abrangente de empresas que operam na União Europeia em todos os setores importantes, reduzir as diferenças em termos de resiliência no mercado interno nos setores já abrangidos pela diretiva, e melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta.

Basear-se-á no que já foi alcançado com a aplicação da Diretiva (UE) 2016/1148 nos últimos quatro anos.

*1.5.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.*

A ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de medidas nacionais ou regionais estanques. A Diretiva SRI surgiu para colmatar esta lacuna, estabelecendo um quadro para a segurança das redes e dos sistemas de informação a nível nacional e da União. No entanto, a primeira avaliação periódica da Diretiva SRI revelou várias deficiências intrínsecas, que acabaram por levar a disparidades consideráveis entre os Estados-Membros em termos de capacidades, planeamento e nível de proteção, e que, ao mesmo tempo, afetam a equidade das condições de concorrência para empresas similares no mercado interno.

A intervenção da UE, indo além das atuais medidas previstas na Diretiva SRI, justifica-se principalmente: i) pelo carácter transfronteiriço do problema; ii) pelo potencial da ação da UE para melhorar e facilitar a eficácia das políticas nacionais; iii) pelo contributo de ações concertadas e colaborativas de política em matéria de SRI para uma proteção eficaz dos dados e da privacidade.

Assim, os objetivos enumerados podem ser mais facilmente alcançados por uma ação a nível da UE do que pelos Estados-Membros agindo isoladamente.

*1.5.3. Ensinamentos retirados de experiências anteriores semelhantes*

A Diretiva SRI é o primeiro instrumento horizontal do mercado interno destinado a melhorar a resiliência das redes e dos sistemas na União contra os riscos de cibersegurança, Desde a sua entrada em vigor, em 2016, já contribuiu, em grande medida, para aumentar o nível comum de cibersegurança entre os Estados-Membros. No entanto, a avaliação do funcionamento e da aplicação da diretiva revelou várias deficiências que, juntamente com a crescente digitalização e a necessidade de uma resposta mais atualizada, devem ser abordadas por via de um ato jurídico revisto.

*1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados*

A nova proposta é inteiramente compatível e coerente com outras iniciativas relacionadas, como a proposta de regulamento relativo à resiliência operacional digital do setor financeiro («DORA») e a proposta de diretiva relativa à resiliência de operadores críticos de serviços essenciais. É também coerente com o Código Europeu das Comunicações Eletrónicas, o Regulamento Geral sobre a Proteção de Dados e o Regulamento eIDAS.

A proposta é uma parte essencial da Estratégia para a União da Segurança.

*1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação*

A gestão destas atribuições por parte da ENISA exige perfis específicos e uma carga de trabalho suplementar que não podem ser absorvidos sem um aumento dos recursos humanos.

## 1.6. Duração e impacto financeiro da proposta/iniciativa

☐ **duração limitada**

– ☐ Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA

☒ **duração ilimitada**

– Aplicação com um período de arranque entre 2022 e 2025,

– seguido de um período de aplicação a um ritmo de cruzeiro.

## 1.7. Modalidade(s) de gestão prevista(s)[57]

☒ **Gestão direta** pela Comissão

através de

– ☐ agências de execução

☐ **Gestão partilhada** com os Estados-Membros

☐X **Gestão indireta**, confiando tarefas de execução orçamental:

☐ a organizações internacionais e respetivas agências (a especificar);

☐ ao BEI e ao Fundo Europeu de Investimento;

☒ aos organismos referidos nos artigos 70.º e 71.º;

☐ a organismos de direito público;

☐ a organismos regidos pelo direito privado com uma missão de serviço público, na medida em que prestem garantias financeiras adequadas;

☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

☐ a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

Observações

A Agência da União Europeia para a Cibersegurança (ENISA), à qual foi conferido um novo mandato permanente pelo Regulamento Cibersegurança, ajudaria os Estados-Membros e a Comissão na aplicação da Diretiva SRI revista.

Como resultado da Diretiva SRI revista, a partir de 2022-2023, a ENISA terá domínios de ação adicionais. Embora estes domínios de ação estejam abrangidos pelas atribuições gerais da ENISA de acordo com o seu mandato, significarão numa carga de trabalho adicional para a agência. Mais precisamente, além dos seus atuais domínios de ação, nos termos da proposta da Comissão de uma Diretiva SRI revista, a ENISA deverá também incorporar especificamente no seu programa de trabalho, nomeadamente, as seguintes ações: i) criar e manter um registo europeu de vulnerabilidades (artigo 6.º, n.º 2, da proposta); ii) assegurar os serviços de secretariado da Rede Europeia de Organizações de Coordenação de Cibercrises (CyCLONe) (artigo 14.º da proposta) e elaborar um relatório anual sobre o

[57] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

estado da cibersegurança na UE (artigo 15.º da proposta); iii) apoiar a organização de análises pelos pares entre Estados-Membros (artigo 16.º da proposta); iv) recolher dados agregados sobre incidentes dos Estados-Membros e emitir orientações técnicas (artigo 20.º, n.º 9, da proposta); v) criar e manter um registo de entidades que prestam serviços transfronteiriços (artigo 25.º da proposta).

Por conseguinte, será apresentado um pedido de 5 ETI suplementares a partir de 2022, com o orçamento correspondente de cerca de 0,61 milhões de EUR por ano, para cobrir estes novos lugares.

## 2. MEDIDAS DE GESTÃO

### 2.1. Disposições em matéria de acompanhamento e comunicação de informações

*Especificar a periodicidade e as condições.*

A Comissão avaliará periodicamente a aplicação da diretiva e apresentará um relatório ao Parlamento Europeu e ao Conselho, a primeira vez três anos após a sua entrada em vigor.

A Comissão avaliará igualmente a transposição correta da diretiva pelos Estados-Membros.

As atividades de acompanhamento e apresentação de relatórios propostas seguirão os princípios delineados no mandato permanente da ENISA ao abrigo do Regulamento (UE) 2019/881 (Regulamento Cibersegurança).

As fontes de dados utilizadas para o acompanhamento previsto seriam principalmente da ENISA, do grupo de cooperação, da rede de CSIRT e das autoridades dos Estados-Membros. Além dos dados obtidos dos relatórios (nomeadamente os relatórios de atividade anuais) da ENISA, do grupo de cooperação e da rede de CSIRT, poderão ser utilizados instrumentos específicos de recolha de dados quando necessário (por exemplo, inquéritos às autoridades nacionais, Eurobarómetro e relatórios da campanha «mês da cibersegurança» e dos exercícios pan-europeus).

### 2.2. Sistema(s) de gestão e de controlo

*2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos*

A unidade da DG CNECT responsável pelo domínio de intervenção fará a gestão da aplicação da diretiva.

No que respeita à gestão da ENISA, o artigo 15.º do Regulamento Cibersegurança apresenta uma lista pormenorizada das competências de controlo do conselho de administração da ENISA.

Nos termos do artigo 31.º do Regulamento Cibersegurança, o diretor executivo da ENISA é responsável pela execução do seu orçamento e o auditor interno da Comissão exerce, em relação à ENISA, os mesmos poderes que exerce em relação aos serviços da Comissão. O conselho de administração da ENISA emite um parecer sobre as contas definitivas da ENISA.

*2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar*

Risco muito baixo, uma vez que o ecossistema da Diretiva SRI já se encontra estabelecido e já abrange a ENISA, que tem um mandato permanente na sequência da entrada em vigor do Regulamento Cibersegurança em 2019.

*2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)*

O aumento orçamental solicitado aplica-se ao título 1 e destina-se a financiar salários, o que significa um risco de erro muito baixo a nível dos pagamentos.

## 2.3. Medidas de prevenção de fraudes e irregularidades

*Especificar as medidas de prevenção e de proteção existentes ou previstas, como, por exemplo, da estratégia antifraude*

As medidas de prevenção e de proteção da ENISA seriam aplicáveis, especificamente:

— O pagamento de qualquer serviço ou estudo solicitado é controlado pelo pessoal da agência antes de ser efetuado, tendo em conta todas as obrigações contratuais, os princípios económicos e as boas práticas financeiras ou de gestão. Serão incluídas disposições antifraude (supervisão, requisitos de informação, etc.) em todos os acordos e contratos celebrados entre a agência e os destinatários de qualquer pagamento;

— Na luta contra a fraude, corrupção e outras atividades ilícitas, aplicam-se, sem quaisquer restrições, as disposições do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho, de 25 de maio de 1999, relativo aos inquéritos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF);

— Nos termos do artigo 33.º do Regulamento Cibersegurança, em 28 de dezembro de 2019, a ENISA aderiu ao Acordo Interinstitucional, de 25 de maio de 1999, entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão das Comunidades Europeias relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF). A ENISA deve adotar, sem demora, as disposições adequadas aplicáveis a todo o seu pessoal.

# 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

## 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

| Rubrica do quadro financeiro plurianual | Rubrica orçamental | Tipo de despesa | Participação | | | |
|---|---|---|---|---|---|---|
| | Número | DD/DND[58] | dos países da EFTA[59] | dos países candidatos [60] | de países terceiros | na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro |
| 2 | 02 10 04 | ./DND | SIM | NÃO | NÃO | /NÃO |

- Novas rubricas orçamentais, cuja criação é solicitada

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

[58] DD = dotações diferenciadas/DND = dotações não diferenciadas.
[59] EFTA: Associação Europeia de Comércio Livre.
[60] Países candidatos e, se aplicável, países candidatos potenciais dos Balcãs Ocidentais.

| Rubrica do quadro financeiro plurianual | Rubrica orçamental | Tipo de despesa | Participação | | | |
|---|---|---|---|---|---|---|
| | Número | DD/DND | dos países da EFTA | dos países candidatos | de países terceiros | na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro |
| | [XX.YY.YY.YY] | | SIM/NÃO | SIM/NÃO | SIM/NÃO | SIM/NÃO |

### 3.2. Impacto estimado nas despesas

*3.2.1. Síntese do impacto estimado nas despesas*

Em milhões de EUR (três casas decimais)

| **Rubrica do quadro financeiro plurianual** | Número | [Rubrica…2 Mercado único, inovação e digital……..……] |
|---|---|---|

| [Organismo]: <…ENISA….> | | | Ano **N**[61] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) **2026** | **2027** | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|
| Título 1: | Autorizações | (1) | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Pagamentos | (2) | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| Título 2: | Autorizações | (1a) | | | | | | | | |
| | Pagamentos | (2 a) | | | | | | | | |
| Título 3: | Autorizações | (3 a) | | | | | | | | |
| | Pagamentos | (3b) | | | | | | | | |
| **TOTAL das dotações para [organismo]** <ENISA…….> | Autorizações | = 1+1a+3 a | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Pagamentos | =2+2a +3b | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |

[61] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

| **Rubrica do quadro financeiro plurianual** | **5** | «Despesas administrativas» |
|---|---|---|

Em milhões de EUR (três casas decimais)

| | | Ano **N** | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| DG: <…….> | | | | | | | | | |
| • Recursos humanos | | | | | | | | | |
| • Outras despesas administrativas | | | | | | | | | |
| **TOTAL DG** <…….> | Dotações | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações no âmbito da RUBRICA 5** do quadro financeiro plurianual | (Total das autorizações = total dos pagamentos) | | | | | | | | |

Em milhões de EUR (três casas decimais)

| | | Ano **N**[62] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) **2026** | **2027** | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações no âmbito das RUBRICAS 1 a 5** do quadro financeiro plurianual | Autorizações | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Pagamentos | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |

[62] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

*3.2.2. Impacto estimado nas dotações do(a) [organismo]*

– ☐x A proposta/iniciativa não acarreta a utilização de dotações operacionais

– ☐ A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

| **Indicar os objetivos e as realizações** ⇩ | | | Ano **N** | | Ano **N+1** | | Ano **N+2** | | Ano **N+3** | | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **REALIZAÇÕES** | | | | | | | | | | | | | | | | | |
| | Tipo[63] | Custo médio | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º total | Custo total |
| OBJETIVO ESPECÍFICO N.º 1[64]… | | | | | | | | | | | | | | | | | | |
| — Realização | | | | | | | | | | | | | | | | | | |
| — Realização | | | | | | | | | | | | | | | | | | |
| — Realização | | | | | | | | | | | | | | | | | | |
| Subtotal objetivo específico n.º 1 | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO N.º 2… | | | | | | | | | | | | | | | | | | |
| — Realização | | | | | | | | | | | | | | | | | | |
| Subtotal objetivo específico n.º 2 | | | | | | | | | | | | | | | | | | |
| **CUSTO TOTAL** | | | | | | | | | | | | | | | | | | |

63 As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

64 Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…».

*3.2.3. Impacto estimado nos recursos humanos da ENISA*

3.2.3.1. Síntese

Como resultado da Diretiva SRI revista, a partir de 2022/23, a ENISA desempenhará funções adicionais. Embora estas funções estejam abrangidas pelo mandato da ENISA, darão origem a uma carga de trabalho adicional para a agência. Mais precisamente, além das suas atuais funções, nos termos da proposta da Comissão de uma Diretiva SRI revista, a ENISA será encarregada, nomeadamente, de: i) criar e manter um registo europeu de vulnerabilidades (artigo 6.º, n.º 2); ii) assegurar os serviços de secretariado da Rede Europeia de Organizações de Coordenação de Cibercrises (CyCLONe) (artigo 14.º) e elaborar um relatório anual sobre o estado da cibersegurança na UE (artigo 15.º); iii) apoiar a organização de análises pelos pares entre Estados-Membros (artigo 16.º); iv) recolher dados agregados sobre incidentes dos Estados-Membros e emitir orientações técnicas (artigo 20.º, n.º 9); v) criar e manter um registo de entidades que prestam serviços transfronteiriços (artigo 25.º).

Por conseguinte, será apresentado um pedido de 5 ETI suplementares a partir de 2022, com o orçamento correspondente para cobrir estes novos lugares.

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– ☐X A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

| | Ano **N**[65] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) **2026** **2027** | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agentes temporários (graus AD) | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | | **2,7** |
| Agentes temporários (graus AST) | | | | | | | | |
| Agentes contratuais | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | | **0,96** |
| Peritos nacionais destacados | | | | | | | | |
| **TOTAL** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | | **3,66** |

65 O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

Necessidades de pessoal (ETI):

| | Ano **N**[66] **2022** | Ano **N+1** **2023** | Ano **N+2** **2024** | Ano **N+3** **2025** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) **2026** | **2027** | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agentes temporários (graus AD) | 3 | 3 | 3 | 3 | 3 | 3 | | **18** |
| Agentes temporários (graus AST) | | | | | | | | |
| Agentes contratuais | 2 | 2 | 2 | 2 | 2 | 2 | | **12** |
| Peritos nacionais destacados | | | | | | | | |
| **TOTAL** | **5** | **5** | **5** | **5** | **5** | **5** | | **30** |

3.2.3.2. Necessidades estimadas de recursos humanos para a DG responsável

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos.

– ☐ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

*As estimativas devem ser expressas em números inteiros (ou, no máximo, com uma casa decimal)*

| | Ano **N** | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | |
|---|---|---|---|---|---|---|---|
| • **Lugares do quadro do pessoal (funcionários e agentes temporários)** | | | | | | | |
| XX 01 01 01 (na sede e nos gabinetes de representação da Comissão) | | | | | | | |
| XX 01 01 02 (nas delegações) | | | | | | | |
| XX 01 05 01 (investigação indireta) | | | | | | | |
| 10 01 05 01 (investigação direta) | | | | | | | |
| | | | | | | | |
| • **Pessoal externo (em equivalente a tempo** | | | | | | | |

[66] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **inteiro: ETI)**[67] | | | | | | | | |
| XX 01 02 01 (AC, PND e TT da «dotação global») | | | | | | | | |
| XX 01 02 02 (AC, AL, PND, TT e JPD nas delegações) | | | | | | | | |
| **XX** 01 04 ***yy***[68] | — na sede[69] | | | | | | | |
| | — nas delegações | | | | | | | |
| **XX** 01 05 02 (AC, PND e TT – Investigação indireta) | | | | | | | | |
| 10 01 05 02 (AC, PND e TT – Investigação direta) | | | | | | | | |
| Outras rubricas orçamentais (especificar) | | | | | | | | |
| **TOTAL** | | | | | | | | |

**XX** constitui o domínio de intervenção ou título em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

| | |
|---|---|
| Funcionários e agentes temporários | |
| Pessoal externo | |

A descrição do cálculo do custo de um ETI deve figurar no anexo V, secção 3.

67 AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

68 Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

69 Principalmente para os fundos estruturais, o Fundo Europeu Agrícola de Desenvolvimento Rural (FEADER) e o Fundo Europeu das Pescas (FEP).

*3.2.4. Compatibilidade com o atual quadro financeiro plurianual*

– ☐X A proposta/iniciativa é compatível com o atual quadro financeiro plurianual.

– ☐ A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual.

| |
|---|
| Explicitar a reprogramação necessária, especificando as rubricas orçamentais em causa e as quantias correspondentes.<br><br>A proposta é compatível com o QFP 2021-2027.<br><br>A compensação do orçamento solicitado para cobrir o aumento dos recursos humanos da ENISA será efetuada pela redução, no mesmo montante, do orçamento do Programa Europa Digital na mesma rubrica. |

– ☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual[70].

| |
|---|
| Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes. |

*3.2.5. Participação de terceiros no financiamento*

– A proposta/iniciativa não prevê o cofinanciamento por terceiros.

– A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

Em milhões de EUR (três casas decimais)

| | Ano **N** | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | Total |
|---|---|---|---|---|---|---|---|---|
| Especificar o organismo de cofinanciamento | | | | | | | | |
| TOTAL das dotações cofinanciadas | | | | | | | | |

[70] Ver os artigos 11.º e 17.º do Regulamento (UE, Euratom) n.º 1311/2013 do Conselho que estabelece o quadro financeiro plurianual para o período 2014-2020.

### 3.3. Impacto estimado nas receitas

– ☐ A proposta/iniciativa não tem impacto financeiro nas receitas.

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

☐ nos recursos próprios

☐ noutras receitas

☐ indicar se as receitas são afetadas a rubricas de despesas

Em milhões de EUR (três casas decimais)

| Rubrica orçamental das receitas: | Dotações disponíveis para o atual exercício | Impacto da proposta/iniciativa[71] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Ano **N** | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | |
| Artigo ……. | | | | | | | | |

Relativamente às diversas receitas «afetadas», especificar a(s) rubrica(s) orçamental(is) de despesas envolvida(s).

Especificar o método de cálculo do impacto nas receitas.

[71] No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.