Conselho da
União Europeia

Bruxelas, 26 de novembro de 2021
(OR. en)

14337/21

Dossiê interinstitucional:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTA

de:	Secretariado-Geral do Conselho
para:	Conselho
n.º doc. ant.:	9583/2/21, 11724/21
n.° doc. Com.:	14150/20
Assunto:	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 2016/1148 – *Orientação geral*

I. INTRODUÇÃO

1. Em 16 de dezembro de 2020, a Comissão adotou a proposta de diretiva Segurança das Redes e da Informação revista (Diretiva SRI revista ou "SRI 2")[1], com o objetivo de substituir a atual Diretiva Segurança das Redes e da Informação ("Diretiva SRI")[2].

[1] 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 2016/1148

[2] Diretiva 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.

A proposta era uma das ações previstas na Estratégia de cibersegurança da UE para a década digital[3] destinadas a garantir que os cidadãos e as empresas beneficiem de tecnologias digitais fiáveis.

2. A proposta baseia-se no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e tem por objetivo continuar a aumentar a resiliência e a capacidade de resposta a incidentes por parte das entidades públicas e privadas, das autoridades competentes e da União no seu conjunto.

3. No Parlamento Europeu, a comissão responsável por esta proposta é a Comissão da Indústria, da Investigação e da Energia (ITRE). A Comissão ITRE adotou o relatório do relator em 28 de outubro de 2021.

4. O Comité Económico e Social Europeu adotou o respetivo parecer em 28 de abril de 2021.

5. Em 3 de fevereiro de 2021, o Comité de Representantes Permanentes decidiu consultar o Comité das Regiões Europeu sobre a proposta[4]. Até à data, este Comité ainda não emitiu parecer.

6. A Autoridade Europeia para a Proteção de Dados adotou parecer em 11 de março de 2021[5].

7. Nas suas conclusões[6] de 22 março de 2021 sobre a Estratégia de Cibersegurança da UE para a década digital, o Conselho tomou nota da nova proposta, que tem por base a Diretiva SRI, e reiterou o seu apoio ao reforço e harmonização dos quadros nacionais de cibersegurança e à cooperação sustentada entre Estados-Membros.

8. Nas suas conclusões de 21-22 de outubro de 2021, o Conselho Europeu apelou a que se impulsionassem os trabalhos sobre a proposta de revisão da Diretiva SRI.

---

3 14133/20
4 5573/21
5 Parecer 5/2021 sobre a Estratégia para a Cibersegurança e a Diretiva SRI 2
6 6722/21

II. TRABALHOS NAS INSTÂNCIAS PREPARATÓRIAS DO CONSELHO

9. No Conselho, a análise da proposta tem sido realizada no Grupo Horizontal das Questões do Ciberespaço (a seguir designado por "Grupo Horizontal"). A análise da proposta teve início durante a Presidência portuguesa, em 19 de janeiro, com uma leitura cuidadosa da proposta, que permitiu aos Estados-Membros fazerem perguntas, apresentarem as suas principais preocupações e obterem explicações detalharas da Comissão sobre as alterações da diretiva revista.

10. Ao longo da Presidência portuguesa, o Grupo Horizontal dedicou 17 reuniões à apresentação e leitura da proposta. A 4 de junho de 2021, foi apresentado ao Conselho TTE um relatório intercalar do exercício de leitura.

11. Desde então, os trabalhos prosseguiram e intensificaram-se ao longo da Presidência eslovena, com o objetivo de se chegar a uma orientação geral na reunião do Conselho (Transportes, Telecomunicações e Energia) de 3 de dezembro de 2021. A Presidência eslovena dedicou 15 reuniões à revisão da proposta de Diretiva SRI 2 e a muitos debates bilaterais a todos os níveis.

12. Num primeiro momento, o Grupo Horizontal centrou o seu trabalho na reformulação do texto da proposta, na interação entre a Diretiva SRI 2 e a legislação setorial e no seu âmbito de aplicação, em especial no que toca à administração pública, aos servidores raiz de DNS e à cláusula de exclusão, e, num segundo momento, concentrou-se, entre outras coisas, nas avaliações pelos pares, nas questões de jurisdição e de assistência mútua, na divulgação coordenada de vulnerabilidades, nas bases de dados dos nomes de domínio e dados de registo e na cooperação internacional.

13. Em 21 de setembro de 2021[7], foi apresentada uma primeira proposta de compromisso relativamente ao texto da proposta de diretiva, tendo por base as observações apresentadas por escrito e os documentos oficiosos enviados pelos Estados-Membros, bem como as anteriores propostas de compromisso no que toca à interação entre a Diretiva SRI 2 e a legislação setorial e ao âmbito de aplicação da Diretiva SRI 2.

---

7 12019/21

14. A última revisão[8] da proposta de compromisso da Presidência foi debatida a nível do Grupo em 22 de novembro de 2021. Embora, de um modo geral, as delegações tenham acolhido favoravelmente o texto de compromisso, algumas delas formularam reservas de análise ou fizeram observações sobre certas partes da proposta de compromisso. Foram ainda sugeridas algumas reformulações de caráter técnico em certas partes do texto.

III. QUESTÕES DE FUNDO

15. Com base nos debates realizados a nível do Grupo, foram identificados como principais questões políticas a resolver os seguintes pontos:

a) Âmbito de aplicação (artigo 2.º)

Desde o início dos debates sobre a proposta de Diretiva SRI 2 que a principal preocupação dos Estados-Membros tem sido o aumento significativo do número de entidades abrangidas pela diretiva e, em especial, a introdução da regra da limitação com base na dimensão, segundo a qual todas as entidades de média e grande dimensão que operam nos setores ou prestam serviços abrangidos pela Diretiva SRI 2 são incluídas no seu âmbito de aplicação. Embora a proposta de compromisso mantenha esta regra geral, inclui também disposições adicionais para assegurar a proporcionalidade necessária, um nível mais elevado de gestão dos riscos e critérios precisos fundamentais para determinar quais as entidades abrangidas pelo âmbito de aplicação da diretiva. Além disso, a proposta de compromisso inclui disposições específicas sobre as prioridades no recurso às medidas de supervisão de acordo com uma abordagem baseada no risco.

[8] 12019/5/21 REV 5

b) Administração pública (artigo 2.º, n.º 2-A)

A inclusão da administração pública no âmbito de aplicação da Diretiva SRI 2 foi um tema altamente debatido, tendo em conta que esse setor tem características bastante diferentes de outros que são abrangidos pela mesma diretiva. A Presidência procurou encontrar uma abordagem equilibrada que tivesse em conta as especificidades dos quadros nacionais da administração pública e que garantisse aos Estados-Membros um certo grau de flexibilidade ao definirem quais as entidades da administração pública que ficam abrangidas pelo âmbito de aplicação da Diretiva. Por conseguinte, embora no texto de compromisso a Diretiva SRI 2 se aplique às entidades da administração pública a nível central, os Estados-Membros podem determinar que esta também se aplica às entidades das administrações regionais e locais.

c) Cláusula de exclusão (artigo 2.º, n.º 3-A e 3-aA)

Os Estados-Membros pretenderam clarificar melhor a cláusula de exclusão, na medida em que a diretiva não se aplica as entidades que exerçam as suas principais atividades nos domínios da defesa, da segurança nacional, da segurança pública ou da aplicação da lei nem às atividades relacionadas com a segurança nacional ou a defesa. O sistema judicial, os parlamentos e os bancos centrais ficam igualmente excluídos.

d) Interação com a legislação setorial

Os Estados-Membros salientaram a necessidade de alinhamento entre a Diretiva SRI 2 e a legislação setorial, nomeadamente o Regulamento relativo à resiliência operacional digital do setor financeiro ("DORA") e a Diretiva relativa à resiliência das entidades críticas (Diretiva REC). A Diretiva SRI 2, que deverá constituir a base para uma harmonização mínima em matéria de cibersegurança, contém um artigo específico sobre atos setoriais da União (artigo 2.º-B). No que diz respeito à interação com a Diretiva RCE, a proposta de compromisso assegura uma maior clareza quanto à abordagem que contempla todos os riscos. Outros aditamentos importantes dizem respeito aos acordos de cooperação entre as autoridades competentes nos termos dos respetivos atos jurídicos.

e) Aprendizagem entre pares (artigo 16.º)

Com algumas exceções, os Estados-Membros opuseram-se a que a Comissão determinasse a realização de análises pelos pares com caráter obrigatório. O compromisso proposto garante que o novo mecanismo de aprendizagem entre pares assenta na confiança mútua e constitui um processo voluntário da iniciativa dos Estados-Membros.

f) Competência e territorialidade (artigo 24.º) e assistência mútua (artigo 34.º)

Os Estados-Membros manifestaram-se preocupados com as consequências de uma competência diferenciada para as entidades do setor das TIC, tal como proposto pela Comissão. O texto de compromisso clarificou as questões de competência com base no tipo de entidades e reforçou a os termos da redação relativa à assistência mútua.

g) Obrigação de notificação (artigo 20.º)

Devido às preocupações manifestadas pelos Estados-Membros, segundo as quais este procedimento sobrecarregaria as entidades abrangidas pela Diretiva SRI 2 e levaria a um excesso de notificações, a comunicação obrigatória de ciberameaças significativas foi excluída do texto de compromisso.

IV. CONCLUSÕES

16. Em 24 de novembro de 2021, o Comité de Representantes Permanentes chegou a acordo sobre o texto de compromisso constante do anexo e decidiu apresentá-lo ao Conselho (Transportes, Telecomunicações e Energia) para adoção de uma orientação geral.

17. Deste modo, solicita-se ao Conselho que aprove o texto de compromisso apresentado pela Presidência, constante do anexo, e adote uma orientação geral na reunião de 3 de dezembro de 2021.

ANEXO

Proposta de

DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO

relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) 910/2014 e a Diretiva (UE) 2018/1972 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,

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

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 [...] **para a segurança das redes e dos sistemas de informação**, 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 "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.

---

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.

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

(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 **medidas** [...] 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 **medidas** [...] 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, 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) [...] Os Estados-Membros **deverão poder** 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 [...]. [...] **A Diretiva não se deverá aplicar a determinadas entidades públicas ou privadas que exerçam atividades nesses domínios. Também não se deverá aplicar às atividades que as entidades realizem nestes domínios. Além disso**, 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 **n**acionais [...] **ou** 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"[14] (Traffic Light Protocol).

(6-A) O direito da União em matéria de proteção de dados pessoais e de privacidade é aplicável a qualquer tratamento de dados pessoais realizado ao abrigo da presente diretiva. Em especial, a presente diretiva não prejudica o Regulamento (UE) 2016/679 nem a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, pelo que, não deverá afetar, em especial, as funções e as competências das autoridades de supervisão independentes competentes em matéria de controlo do cumprimento da legislação da União sobre proteção de dados.

---

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.

(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. [...]

[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).

(8-A) A fim de obter uma panorâmica clara de quais as entidades abrangidas pelo âmbito de aplicação da presente diretiva, os Estados-Membros deverão poder estabelecer mecanismos nacionais de autonotificação que exijam às entidades abrangidas pela presente diretiva que indiquem às autoridades competentes nos termos da presente diretiva ou aos organismos designados para o efeito pelos Estados-Membros, no mínimo, o seu nome, endereço e outros dados de contacto, bem como o setor no qual operam ou o tipo de serviço que prestam e, se for o caso, uma lista dos Estados--Membros onde as entidades prestam serviços. Se existirem registos a nível nacional, os Estados-Membros podem decidir quais são os mecanismos adequados para identificar as entidades abrangidas pelo âmbito de aplicação da presente diretiva.

(9) [...] **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 responsáveis por [...] apresen**tar** [...] à Comissão **pelo menos as informações relevantes quanto ao número de entidades identificadas, ao setor a que pertencem ou ao tipo de serviço que prestam, assim como aos critérios específicos com base nos quais foram identificadas. Os Estados-Membros podem também decidir, caso as regras nacionais de segurança assim o prevejam, apresentar à Comissão os nomes dessas entidades.**

(9-A) Ficam excluídos do âmbito de aplicação da presente diretiva as entidades da administração pública que exerçam atividades nos domínios da segurança nacional, da defesa, da segurança pública e da aplicação da lei, bem como o sistema judicial, os parlamentos e os bancos centrais. Para efeitos da presente diretiva, não se considera que as entidades com competência regulamentar exercem atividades no domínio da aplicação da lei, pelo que não ficam por esse motivo excluídas do âmbito de aplicação da presente diretiva. Além disso, as entidades da administração pública da administração central estabelecidas em conjunto com um país terceiro nos termos de um acordo internacional não são abrangidas pelo âmbito de aplicação da presente diretiva.

(9-AA)Os Estados-Membros deverão poder determinar que as entidades identificadas como operadores de serviços essenciais antes da entrada em vigor da presente diretiva, nos termos da Diretiva (UE) 2016/1148, deverão ser consideradas entidades essenciais.

(9-AAA) A presente diretiva não se aplica às missões diplomáticas e consulares dos Estados--Membros no estrangeiro nem às infraestruturas de TIC utilizadas por tais missões, na medida em que essas infraestruturas estejam localizadas no estrangeiro ou sejam exploradas para utilizadores no estrangeiro.

(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) [...] **As entidades abrangidas pelo âmbito de aplicação da presente diretiva deverão ser classificadas em duas categorias: essenciais e importantes, em função do grau de importância do setor ou do tipo de serviço que prestam, e da sua dimensão. A este respeito, devem também ser tidas devidamente em conta quaisquer avaliações de risco setoriais relevantes ou orientações emitidas pelas autoridades competentes, se for o caso.** Tanto as entidades essenciais como as entidades importantes devem estar sujeitas aos [...] aos 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 os requisitos **baseados no risco** e as obrigações, por um lado, e os encargos administrativos decorrentes da supervisão do cumprimento, por outro.

(12) **A presente diretiva estabelece a base de referência para as medidas de gestão dos riscos de cibersegurança e as obrigações de notificação em todos os setores abrangidos pelo respetivo âmbito de aplicação. A fim de evitar a fragmentação das disposições em matéria de cibersegurança dos atos jurídicos da União, sempre que se considerem necessárias disposições setoriais adicionais relativas** às medidas de gestão dos riscos de cibersegurança **e às obrigações de notificação para garantir um elevado nível de cibersegurança, a Comissão deverá avaliar se essas disposições podem ser definidas num ato de execução adotado em conformidade com as competências previstas na presente diretiva. Caso esses atos não sejam adequados para o efeito**, a legislação setorial **poderá** contribuir para assegurar **um** elevado nível [...] de cibersegurança, tomando simultaneamente em plena consideração as especificidades e complexidades [...] **dos** setores **em causa**. **O motivo pelo qual se considerou inadequado um ato de execução adotado em conformidade com as competências previstas na presente diretiva deverá ser exposto na legislação setorial específica. Ao mesmo tempo, as disposições setoriais dos atos jurídicos da União deverão ter devidamente em conta a necessidade de dispor de um quadro abrangente e harmonizado em matéria de cibersegurança.** [...] Isto [...] não prejudica as atuais competências de execução atribuídas [...] **à** Comissão em vários setores, incluindo os transportes e energia.

(12-A) Nos casos em que [...] atos jurídicos setoriais da União **contenham disposições** que [...] **exijam** que entidades essenciais ou importantes [...] adotem **medidas pelo menos equivalentes às obrigações estabelecidas na presente diretiva no que respeita à** gestão dos riscos de cibersegurança [...] **e à obrigação** de notificação de incidentes ou [...] ciberameaças **significativos** [...], deverão aplicar-se essas disposições setoriais, **incluindo em matéria de supervisão e execução coerciva**. **Ao determinar o efeito equivalente das obrigações estabelecidas nas disposições setoriais de um ato jurídico da União, deverão ser tidos em conta os seguintes aspetos: i) as medidas de gestão dos riscos de cibersegurança deverão compreender medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que as entidades relevantes utilizam na prestação dos seus serviços, e deverão incluir, no mínimo, todos os elementos previstos na presente diretiva; ii) a obrigação de notificar incidentes e ciberameaças significativos deverá ser pelo menos equivalente às obrigações estabelecidas na presente diretiva no que diz respeito ao conteúdo, ao formato e aos prazos das notificações; iii) as modalidades de comunicação dos atos jurídicos setoriais da União pelas entidades e pelas autoridades competentes deverão ser pelo menos equivalentes às obrigações estabelecidas na presente diretiva no que diz respeito ao seu conteúdo, formato e prazos, e deverão ter em conta o papel das CSIRT; iv) os requisitos de cooperação transfronteiras aplicáveis às autoridades competentes deverão ser pelo menos equivalentes aos estabelecidos na presente diretiva. Se as disposições setoriais de um ato jurídico da União não abrangerem todas as entidades de um setor específico que se insira no âmbito de aplicação da presente diretiva, as disposições pertinentes da presente diretiva deverão continuar a aplicar-se às entidades não abrangidas por tais disposições setoriais.**

(12-AA) A Comissão **deverá rever periodicamente a aplicação dos requisitos de efeito equivalente previstos em relação às disposições setoriais dos atos jurídicos da União** [...]. **A Comissão deverá consultar o grupo de cooperação aquando da preparação da revisão periódica.**

(12-AAA) Os futuros atos jurídicos setoriais da União deverão ter devidamente em conta as definições constantes do artigo 4.º e o quadro de supervisão e execução coerciva estabelecido no capítulo VI da presente diretiva.

(12-AB) Nos casos em que as disposições setoriais dos atos jurídicos da União exijam que entidades essenciais ou importantes adotem medidas de efeito pelo menos equivalente às obrigações de notificação estabelecidas na presente diretiva, deverá ser evitada a duplicação de obrigações de notificação e assegurada a coerência e a eficácia do tratamento das notificações de ameaças ou incidentes cibernéticos. Para esse efeito, as referidas disposições setoriais podem permitir que os Estados-Membros criem um mecanismo comum, automático e direto para a comunicação de ameaças e incidentes cibernéticos significativos, tanto às autoridades cujas funções estão definidas nas disposições setoriais respetivas como às autoridades competentes, incluindo ao ponto de contacto único e às CSIRT, consoante o caso, responsáveis pelas tarefas de cibersegurança previstas na presente diretiva, ou por um mecanismo que assegure a partilha sistemática e imediata de informações e a cooperação entre as autoridades competentes e as CSIRT no que diz respeito ao tratamento das notificações. Para efeitos de simplificação das notificações e da aplicação do mecanismo comum, automático e direto para a notificação de incidentes, os Estados-Membros podem, em conformidade com as legislações setoriais, utilizar o ponto de entrada único que estabeleçam nos termos do artigo 11.º, n.º 5-A, da presente diretiva. A fim de assegurar a harmonização, as obrigações em matéria de notificação previstas nos atos jurídicos setoriais da União deverão ser alinhadas pelas especificadas na presente diretiva. Os Estados-Membros podem determinar que as autoridades competentes nos termos da presente diretiva ou as CSIRT nacionais são as destinatárias das notificações, em conformidade com as legislações setoriais.

(13) O Regulamento XXXX/XXXX do Parlamento Europeu e do Conselho 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 e de 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 [...] as autoridades europeias de supervisão (AES) do setor financeiro e as autoridades nacionais competentes ao abrigo do Regulamento XXXX/XXXX [...] participem **nos** [...] **trabalhos** [...] 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 informações pormenorizadas sobre incidentes graves relacionados com as TIC **e ciberameaças significativas** aos pontos de contacto únicos**, às autoridades competentes ou às CSIRT nacionais** designadas nos termos da presente diretiva. **Tal será possível através do envio automático e direto de notificações de incidentes ou através de uma plataforma comum para notificações.** 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.

(13-A) A fim de evitar lacunas e duplicações das obrigações em matéria de cibersegurança impostas às entidades do setor da aviação a que se refere o anexo I, ponto 2, alínea a), as autoridades nacionais designadas nos termos do Regulamento (CE) n.º 300/2008[16] e do Regulamento (UE) 2018/1139[17] do Parlamento Europeu e do Conselho e as autoridades competentes nos termos da presente diretiva deverão cooperar na aplicação de medidas de gestão dos riscos de cibersegurança e na supervisão dessas medidas a nível nacional. O cumprimento das medidas de gestão dos riscos de cibersegurança previstas na presente diretiva [...] por parte de uma entidade poderá ser considerado pelas autoridades nacionais designadas nos termos do Regulamento (CE) n.º 300/2008 e do Regulamento (UE) 2018/1139 como equivalente ao cumprimento dos requisitos estabelecidos nesses regulamentos e nos atos delegados e de execução pertinentes adotados nos termos desses regulamentos.

---

16 **Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008,relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que**

revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

17 **Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1).**

(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 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 c**ompetentes [...]referidas nas duas diretivas deverão cooperar e trocar informações, especialmente no que respeita à identificação de entidades críticas, ciberameaças, riscos de cibersegurança e incidentes, **bem como riscos, ameaças e incidentes não relacionados com a cibersegurança**, que afetem entidades críticas **[**ou **entidades equivalentes a entidades críticas],** [...] **inclusive** sobre medidas **físicas** e de cibersegurança adotadas pelas entidades críticas **e os resultados das atividades de supervisão realizadas em relação a essas entidades. Além disso, a fim de racionalizar as atividades de supervisão entre as autoridades competentes designadas nos termos de ambas as diretivas, e de minimizar os encargos administrativos para as entidades em causa, as autoridades competentes deverão procurar harmonizar os modelos de notificação de incidentes e os processos de supervisão.** [...] **Quando se justificar,** as autoridades competentes ao abrigo da Diretiva (UE) XXXX/XXXX [...] **podem solicitar** às autoridades competentes nos termos da presente diretiva [...] que exerçam os seus poderes de supervisão e execução [...] **em relação a** uma entidade essencial identificada como crítica. [...]

(14-A) As entidades pertencentes ao setor das infraestruturas digitais baseiam-se por natureza nas redes e nos sistemas de informação, pelo que as obrigações impostas a essas entidades pela presente diretiva deverão atender de forma abrangente à segurança física desses sistemas, no quadro das suas obrigações em matéria de gestão dos riscos de cibersegurança e de notificação. Uma vez que essas matérias são abrangidas pela presente diretiva, as obrigações estabelecidas nos capítulos III a VI da Diretiva (UE) XXX/XXX [REC] não se aplicam a tais entidades.

(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 deverá ser aplicável a todos os prestadores de serviços de DNS ao longo da cadeia de **fornecimento e** de resolução de DNS **que são importantes para o mercado interno,** incluindo [...], os de **registos** de nomes de domínio de topo [...], **as entidades que prestam serviços de registo de nomes de domínio, os operadores de** servidores de nomes com autoridade para nomes de domínio e **os operadores de** servidores recursivos. **O termo "prestador de serviços de DNS" não se deverá aplicar aos serviços de DNS operados para fins próprios da entidade em causa e das entidades suas afiliadas. As obrigações em matéria de cibersegurança decorrentes da presente diretiva para esta categoria de prestadores de serviços ficam estritamente limitadas às medidas de gestão dos riscos de cibersegurança e às notificações, pelo que não prejudicam a governação mundial do DNS pela comunidade multipartidária.**

(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 serviço de computação em nuvem incluem, entre outras, as infraestruturas como serviço (IaaS), a plataforma como serviço (PaaS), o *software* como serviço (SaaS) e a rede como serviço (NaaS).** 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 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], [...] **incluindo** [...] os prestadores [...] de serviços de correio expresso, deverão 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.

(**20-A**) **A fim de alcançar e manter um elevado nível de cibersegurança, as estratégias nacionais de cibersegurança exigidas pela presente diretiva deverão compreender quadros coerentes que prevejam uma governação no domínio da cibersegurança. Estas estratégias podem ser compostas por um ou vários documentos de natureza legislativa ou não legislativa.**

(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 deverão receber as notificações de incidentes efetuadas pelas entidades de forma eficaz e eficiente**, também com vista a facilitar, se for o caso, uma resposta atempada a incidentes e a dar uma resposta à entidade notificadora.** Os pontos de contacto únicos deverão ser incumbidos do reencaminhamento das notificações de incidentes para os pontos de contacto únicos de outros Estados-Membros afetados. [...]

(23-A) Os atos jurídicos setoriais da União que exijam medidas de gestão dos riscos de cibersegurança ou obrigações de notificação pelo menos equivalentes às estabelecidas na presente diretiva poderão prever que as autoridades competentes neles designadas exerçam as suas competências de supervisão e execução em relação a essas medidas ou obrigações com a assistência das autoridades competentes designadas nos termos da presente diretiva. As autoridades competentes em causa poderão estabelecer acordos de cooperação para o efeito. Tais acordos de cooperação poderão especificar, entre outros, os procedimentos relativos à coordenação das atividades de supervisão, incluindo os procedimentos das investigações e inspeções no local, em conformidade com o direito nacional e um mecanismo de intercâmbio de informações relevantes entre as autoridades competentes em matéria de supervisão e execução coerciva, incluindo o acesso a informações relacionadas com o ciberespaço solicitadas pelas autoridades competentes designadas nos termos da presente diretiva.

(24) Os Estados-Membros deverão 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, deverão 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 [...] **podem** 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 deverão 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 informação utilizados para prestarem os seus serviços. **Consoante o caso,** os Estados-Membros deverão procurar garantir que todas as CSIRT setoriais possuam o mesmo nível de capacidades técnicas. Os Estados-Membros podem 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 deverão poder participar em redes de cooperação internacional, em complemento da rede de CSIRT criada pela presente diretiva. **Por conseguinte, as CSIRT e as autoridades competentes poderão trocar informações, nomeadamente dados pessoais, com as CSIRT de países terceiros ou com as suas autoridades para efeitos do exercício das suas funções em conformidade com o Regulamento (UE) 2016/679. Na falta de uma decisão de adequação adotada em conformidade com o artigo 45.º do Regulamento (UE) 2016/679 ou de garantias adequadas nos termos do artigo 46.º do mesmo regulamento, o intercâmbio de dados pessoais considerado necessário para efeitos de atenuação de ciberameaças significativas e de resposta a um incidente significativo em curso poderá ser considerado importante razão de interesse público na aceção do artigo 49.º, n.º 1, alínea d), do Regulamento (UE) 2016/679.**

---

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).

(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 **ou administram** esses sistemas deverão, 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 deverá adotar igualmente os procedimentos necessários para receber informações sobre vulnerabilidades fornecidas por terceiros. Nesta matéria, as normas internacionais ISO/IEC 30111 e ISO/IEC [...] **29147** 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 coordenação entre a entidade notificadora e a organização no que respeita ao momento da correção e da publicação das vulnerabilidades.

---

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).

(29) Por conseguinte, os Estados-Membros deverão tomar medidas para facilitar a divulgação coordenada de vulnerabilidades, definindo uma política nacional nessa matéria. **No âmbito da sua política nacional, os Estados-Membros deverão procurar resolver, na medida do possível, os problemas encontrados pelos peritos que investigam as vulnerabilidades, nomeadamente a sua potencial incorrência em responsabilidade penal, em conformidade com a respetiva ordem jurídica nacional.** [...] Os Estados-Membros deverão 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 deverão 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 das vulnerabilidades que afetem várias organizações (divulgação **coordenada** de vulnerabilidades a várias partes). Sempre que **a** vulnerabilidade **comunicada possa ter repercussões significativas para as entidades** [...] de mais do que um Estado-Membro, as CSIRT designadas [...] deverão cooperar no âmbito da rede de CSIRT**, se tal se justificar**.

(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 deverá 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 **ou CSIRT designadas**, possam, a título voluntário, divulgar vulnerabilidades e fornecer as informações conexas que permitam aos utilizadores tomar 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. **Em particular, a ENISA deverá explorar a possibilidade de estabelecer uma estreita cooperação com os operadores do sistema de Vulnerabilidades e Exposições Comuns (CVE), incluindo a possibilidade de passar a ser uma autoridade de numeração de raiz do CVE.**

(32) **O grupo de cooperação deverá continuar a apoiar e a facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros, bem como a reforçar a confiança entre eles.** O grupo de cooperação deverá 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 deverá 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 deverá 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 deverão estar habilitadas a participar em programas de intercâmbio de funcionários com outros Estados-Membros, no intuito de reforçar a cooperação. As autoridades competentes deverão tomar as medidas necessárias para permitir que os funcionários de outros Estados-Membros participem ativamente nas atividades da autoridade competente de acolhimento.

(35-A) A rede de CSIRT deverá continuar a contribuir para reforçar a confiança e a promover uma cooperação operacional rápida e eficaz entre os Estados-Membros. A fim de reforçar a cooperação operacional a nível da União, a rede de CSIRT deverá ponderar a possibilidade de convidar os organismos e as agências da União implicados na política de cibersegurança, como a Europol, a participar nos seus trabalhos.

(36) [...]

(36-A) A fim de facilitar a aplicação efetiva das disposições da presente diretiva, tais como a gestão de vulnerabilidades, a gestão dos riscos em matéria de cibersegurança, as medidas de comunicação de informações e os mecanismos de partilha de informações, os Estados-Membros podem cooperar com países terceiros e empreender atividades que considerem adequadas para esse efeito, nomeadamente no domínio do intercâmbio de informações sobre ameaças, bem como dos incidentes, vulnerabilidades, ferramentas e métodos, táticas, técnicas e procedimentos, grau de preparação e exercícios de gestão de cibercrises, formação, criação de confiança e mecanismos estruturados de partilha de informações. Tais acordos de cooperação deverão respeitar o direito da União em matéria de proteção de 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 **Europeia** 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 deverão cooperar com base em disposições processuais que definam as modalidades dessa cooperação **e evitar qualquer duplicação de tarefas.** O regulamento interno da UE-CyCLONe deverá 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 **político** da União, as partes responsáveis deverão recorrer ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR). A Comissão deverá 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), deverá ser ativado o mecanismo de resposta a situações de crise (CRM) do Serviço Europeu para a Ação Externa (SEAE).

(37-A) A EU-CyCLONe deverá funcionar como uma rede intermediária entre o nível técnico e político durante incidentes e crises de cibersegurança em larga escala. Deverá reforçar a cooperação a nível operacional, com base nas conclusões da rede de CSIRT e utilizando capacidades próprias para elaborar análises de impacto dos incidentes e crises de grande escala e apoiar a tomada de decisões a nível político. As instituições, organismos e agências da UE deverão nomear uma autoridade competente responsável pela gestão de crises e incidentes de segurança de grande escala para integrar a EU-CyCLONe.

(38) [...]

(39) [...]

(39-A) A responsabilidade de garantir a segurança das redes e do sistema de informação cabe, em larga medida, às entidades essenciais e importantes. Dever-se-á promover e desenvolver uma cultura de gestão de riscos que passe pela avaliação dos riscos e pela aplicação de medidas de segurança adequadas aos riscos enfrentados.

(40) As medidas de gestão de riscos deverão **ter em consideração o grau de dependência da entidade em relação às redes e aos sistemas de informação e** 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.

(40-A) Uma vez que as ameaças à segurança das redes e dos sistemas de informação podem ter origens diferentes, a presente diretiva segue uma abordagem que contempla todos os riscos e compreende a proteção das redes e dos sistemas de informação e do seu ambiente físico contra qualquer evento, como o roubo, incêndio, inundação, falhas de telecomunicações ou de energia, ou contra qualquer acesso físico não autorizado, bem como danos causados e interferências praticadas nas instalações de tratamento de informações da entidade, que possa comprometer a disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos pelas redes e sistemas de informação ou a que estes deem acesso. Por conseguinte, as medidas de gestão dos riscos deverão também resolver problemas de segurança física e ambiental, incluindo para tal medidas para proteger a rede e os sistemas de informação da entidade contra falhas do sistema, erros humanos, ações maliciosas ou fenómenos naturais, em conformidade com as normas europeias ou internacionalmente reconhecidas, como as que integram a série ISO 27000. A este respeito, as entidades deverão, no quadro das suas medidas de gestão dos riscos, atender também à segurança dos recursos humanos e dispor de políticas adequadas de controlo do acesso. Essas medidas deverão ser coerentes com a Diretiva XXXX [Diretiva RCE].

(40-B) Na falta de sistemas europeus adequados de certificação da cibersegurançcas, adotados nos termos do Regulamento (UE) 2019/881, os Estados-Membros poderão exigir que as entidades utilizem produtos, serviços e processos de TIC certificados ou que obtenham um certificado no quadro dos sistemas nacionais de cibersegurança existentes para efeitos do cumprimento dos requisitos de gestão dos riscos de cibersegurança estabelecidos na presente diretiva.

(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 deverão ser proporcionados em relação ao risco que representam [...] **para as** redes e o sistema de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas **e os custos da sua aplicação**. **Deverá também ser tida devidamente em conta a dimensão da entidade, bem como a probabilidade de ocorrência de incidentes e a sua gravidade.**

(41-A) A fim de aliviar os encargos regulamentares, os requisitos a cumprir para a aplicação de medidas de gestão dos riscos de cibersegurança para as entidades de média, pequena ou micro dimensão deverão, em princípio, ser menos exigentes, a menos que critérios de criticidade ou avaliações de risco nacionais justifiquem requisitos mais rigorosos, em especial no que diz respeito às entidades que cumprem os critérios de criticidade estabelecidos na presente diretiva.

(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.

(42-AA) Tendo em conta a sua natureza transfronteiriça, os prestadores de serviços do sistema de nomes de domínio, os operadores de registo de nomes de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio para domínios de topo, os prestadores de serviços de computação em nuvem, os prestadores de serviços de centros de dados, os fornecedores de redes de distribuição de conteúdos, os prestadores de serviços geridos e os prestadores de serviços de segurança geridos deverão estar sujeitos a um maior grau de harmonização a nível da União. A aplicação de medidas de cibersegurança deverá, por conseguinte, ser facilitada por um ato de execução.

(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 deverão 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 deverão, assim, exercer uma diligência acrescida ao selecionarem um prestador de serviços de segurança geridos.

(44-A) As autoridades nacionais competentes podem também, no contexto das suas funções de supervisão, recorrer a serviços de cibersegurança, tais como auditorias de segurança, testes de penetração ou resposta a incidentes. Para ajudar as entidades, bem como as autoridades nacionais competentes, na seleção de prestadores de serviços de cibersegurança qualificados e fiáveis, a Comissão deverá, com a assistência do grupo de cooperação e da ENISA, ponderar a possibilidade de solicitar o estabelecimento de sistemas europeus de certificação da cibersegurança, em conformidade com o artigo 48.º do Regulamento (UE) 2019/881.

(45) As entidades deverão 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 deverão 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 deverão 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, deverá 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.

[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).

(47) Dadas as características do setor em causa, as avaliações dos riscos associados às cadeias de fornecimento deverão 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 deverão 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 **esses** tipos de entidades.

---

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).

(48-A) As obrigações em matéria de segurança estabelecidas na presente diretiva deverão ser consideradas complementares dos requisitos impostos aos prestadores de serviços de confiança nos termos do Regulamento (UE) n.º 910/2014 (Regulamento eIDAS). Os prestadores de serviços de confiança deverão ser obrigados a tomar todas as medidas adequadas e proporcionadas para gerir os riscos que se colocam aos seus serviços, nomeadamente em relação a clientes e a utilizadores terceiros, e a comunicar incidentes de segurança nos termos da presente diretiva. Tais obrigações em matéria de segurança e de notificação deverão também dizer respeito à proteção física do serviço prestado. Continua a ser aplicável o artigo 24.º do Regulamento (UE) n.º 910/2014.

(48-AA) Os Estados-Membros podem atribuir as funções de autoridade competentes pelos serviços de confiança às entidades supervisoras do eIDAS, a fim de assegurar a continuidade das práticas atuais e tirar partido dos conhecimentos e da experiência resultantes da aplicação do Regulamento eIDAS. Nos casos em que essas funções forem atribuídas a um organismo diferente, as autoridades nacionais competentes nos termos da presente diretiva deverão cooperar estreitamente, em tempo útil, trocando informações relevantes, a fim de assegurar uma supervisão eficaz e o cumprimento dos requisitos estabelecidos na presente diretiva e no Regulamento [XXXX/XXXX] pelos prestadores de serviços de confiança.

Quando se justifique, a autoridade nacional competente nos termos da presente diretiva deverá informar de imediato a entidade supervisora do eIDAS de qualquer ameaça ou incidente cibernético significativo notificado com impacto nos serviços de confiança, bem como de qualquer incumprimento dos requisitos previstos na presente diretiva por parte de prestadores de serviços de confiança. Para efeitos de notificação, os Estados-Membros podem, se for o caso, recorrer ao ponto de entrada único estabelecido para efetuar a comunicação comum e automática de incidentes tanto à entidade supervisora do eIDAS como à autoridade competente nos termos da presente diretiva. 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].

---

[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

(49) Quando adequado e para evitar perturbações desnecessárias, as orientações nacionais em vigor [...] adotadas para efeitos de transposição das regras relacionadas com as medidas de segurança estabelecidas nos artigos 40.º[...] e 41.º da Diretiva (UE) 2018/1972[...] **deverão ser tidas em conta nas disposições de transposição aplicadas pelos Estados-Membros no contexto da presente diretiva, com base nos conhecimentos e competências já adquiridos no âmbito das notificações de risco de acidentes e de segurança nos termos da Diretiva (UE) 2018/1972 no que respeita às medidas de gestão de riscos para a segurança e às notificações de incidentes. A ENISA pode também elaborar orientações para os requisitos em matéria de segurança e notificação destinados aos fornecedores de redes de comunicações eletrónicas públicas ou aos prestadores de serviços de comunicações eletrónicas acessíveis ao público, a fim de facilitar a harmonização e a transição e de minimizar as perturbações. Os Estados-Membros podem atribuir as funções de autoridade competente pelas comunicações eletrónicas às entidades reguladoras nacionais, a fim de assegurar a continuidade das práticas atuais e tirar partido dos conhecimentos e da experiência resultantes da aplicação da Diretiva (EU) 2018/1972.**

(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.

---

eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

(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 deverão informar os destinatários dos seus serviços sobre [...] medidas especiais que possam tomar para minimizar o risco resultante **de uma ciberameaça significativa** a que estejam expostos. **As entidades deverão, sempre que for adequado e, em especial, nos casos em que a ameaça cibernética significativa se possa concretizar, notificar também da própria ameaça os respetivos destinatários de serviços em paralelo com as autoridades competentes ou as CSIRT.** 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 sobre **ciberameaças**[...] à segurança aos destinatários deverá 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, deverá ser promovida e, se necessário, deverá 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 deverá 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 deverão 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 deverão 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 deverá 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 deverá indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso. Os Estados-Membros deverão 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 deverão 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.

(55-A) Uma abordagem proativa das ciberameaças é uma componente vital da gestão dos riscos de cibersegurança que deverá dar às autoridades competentes condições para impedirem eficazmente que as ciberameaças se transformem em incidentes concretos suscetíveis de causar perdas materiais ou imateriais consideráveis. Para o efeito, reveste-se de uma importância fundamental a notificação de ciberameaças significativas.

(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 [...] **poderão** 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, deverá 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) deverão recolher dados relativos ao registo de nomes de domínio e garantir a integridade e disponibilidade desses dados. **No que diz respeito aos dados de registo, as entidades deverão, em especial, verificar o nome e o endereço eletrónico do requerente de registo.** [...] Os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos deverão 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 deverão 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 deverão 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, como é o caso das autoridades competentes nos termos do direito da União ou do direito nacional em matéria de segurança do Estado e de justiça penal ou das CSIRT**. 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. **Os Estados-Membros deverão assegurar que todos os tipos de acesso aos dados de registo de domínio (tanto pessoais como não pessoais) sejam gratuitos.** 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 **em conformidade e complementaridade com as normas internacionais elaboradas pela comunidade multilateral**.

---

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) As entidades [...] **essenciais** e importantes abrangidas pela presente diretiva estão sob a jurisdição do Estado-Membro onde prestam os seus serviços. **Considera-se que as entidades referidas nos pontos 1 a 7 e 10 do anexo I, os prestadores de serviços de confiança e os fornecedores de pontos de troca de tráfego referidos no ponto 8 do anexo I e nos pontos 1 a 5 do anexo II estão sob a jurisdição do Estado-Membro em cujo território tais entidades se encontram estabelecidas.** Se a entidade prestar serviços **ou tiver um estabelecimento** em mais do que um Estado-Membro, deverá estar sob a jurisdição separada e concorrente de cada um desses Estados-Membros. As autoridades competentes desses Estados-Membros deverão cooperar, prestar assistência mútua e, se for o caso, realizar ações de supervisão conjuntas. **Caso decidam exercer a sua jurisdição, os Estados-Membros deverão evitar que o mesmo comportamento seja sancionado mais do que uma vez pelo incumprimento das obrigações estabelecidas na presente diretiva.**

(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, **das entidades que prestam serviços de registo de nomes de domínio para o 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 deverão 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 deverá 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 **predominantemente** tomadas na União. Em regra, corresponderá ao local onde se situa a administração central das empresas na União. Se **o local onde essas decisões são predominantemente tomadas não puder ser determinado ou** tais decisões não forem tomadas na União, deverá considerar-se que o estabelecimento principal se situa no Estado-Membro em que a entidade tem o estabelecimento com o maior número de trabalhadores na União. Se os serviços forem prestados por um grupo de empresas, deverá considerar-se que o seu estabelecimento principal é o estabelecimento principal da empresa que exerce o controlo.

(64-A) Quando o serviço de DNS recursivo é prestado por um fornecedor de redes de comunicações eletrónicas ou por um prestador de serviços de comunicações eletrónicas acessíveis ao público apenas no quadro do serviço de acesso à Internet, deverá considerar-se que a entidade se encontra sob a jurisdição de todos os Estados-Membros em que os seus serviços são prestados.

(64-AA) A fim de assegurar uma panorâmica clara dos prestadores de serviços de DNS, operadores de registos de nomes de domínio de topo, entidades que prestam serviços de registo de nomes de domínio para o TLD, fornecedores de redes de distribuição de conteúdos, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados e prestadores de serviços digitais por toda a União nos termos da presente diretiva, a ENISA deverá criar e conservar um registo para essas entidades, com base nas notificações que os Estados-Membros tenham recebido, se for o caso por intermédio dos seus mecanismos nacionais de autonotificação. A fim de garantir a exatidão e a exaustividade das informações que deverão ser incluídas no referido registo, os Estados-Membros deverão apresentar à ENISA as informações sobre essas entidades existentes nos seus registos nacionais. A ENISA e os Estados-Membros deverão tomar medidas para facilitar a interoperabilidade desses registos, assegurando simultaneamente a proteção das informações confidenciais ou classificadas.

(65) Nos casos em que um prestador de serviços de DNS, um operador de 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, deverá 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) [...]**Na** medida estritamente necessária e proporcionada para garantir a segurança da rede e das informações**, o tratamento de dados pessoais** por entidades **essenciais e importantes** [...] e fornecedores de tecnologias e serviços de segurança **poderá ser considerado necessário para o cumprimento de uma obrigação jurídica ou** [...] constituir um interesse legítimo do responsável pelo tratamento de dados em causa**[...]**, tal como referido no Regulamento (UE) 2016/679. Tal **poderá** [...] 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 [...] de **vários** tipos de dados pessoais**, tais como**: endereços IP, localizadores uniformes de recursos (URL), nomes de domínio e endereços de correio eletrónico. **O tratamento de dados pessoais pelas autoridades competentes, pelos pontos únicos de contacto e pelas CSIRT deverá ser estabelecido no direito nacional e considerado necessário para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento dos dados, tal como se refere no artigo 6.º, n.º 1, alíneas c) ou e), do Regulamento (UE) 2016/679.**

(69-A) A legislação dos Estados-Membros pode estabelecer regras que permitam às autoridades competentes, aos pontos únicos de contacto e às CSIRT, na medida do estritamente necessário e proporcionado para garantir a segurança das redes e dos sistemas de informação de entidades essenciais e importantes, tratar categorias especiais de dados pessoais em conformidade com o artigo 9.º[...] do Regulamento (UE) 2016/679, em especial prevendo medidas adequadas e específicas para salvaguardar os direitos e interesses fundamentais das pessoas singulares, incluindo limitações técnicas à reutilização desses dados e o recurso a medidas de segurança de ponta e a medidas de preservação da privacidade, como a pseudonimização ou a cifragem, caso a anonimização possa afetar de forma significativa a finalidade pretendida.

(70) A fim de reforçar as ações e os poderes de supervisão que ajudam a assegurar um cumprimento efetivo, a presente diretiva deverá estabelecer uma lista mínima de meios e ações de supervisão por meio dos quais as autoridades competentes **podem** [...] 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 deverão ficar sujeitas a um regime de supervisão completo (*ex ante* e *ex post*), ao passo que as entidades importantes deverão ficar sujeitas a um regime de supervisão simplificado, aplicável apenas *ex post*. Tal significa que as entidades importantes não deverão **ser 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. **No caso das entidades importantes, a supervisão *ex-post* pode ser desencadeada por elementos de prova ou quaisquer indicações ou informações levadas ao conhecimento das autoridades competentes que estas considerem sugerir um potencial incumprimento das obrigações estabelecidas na presente diretiva. Por exemplo, esses elementos de prova, indicações ou informações poderão ser do tipo fornecido às autoridades competentes por outras autoridades, entidades, cidadãos, meios de comunicação social ou outras fontes, informações acessíveis ao público, ou poderão resultar de outras atividades realizadas pelas autoridades competentes no exercício das suas funções.**

(70-A) No exercício da supervisão *ex-ante*, as autoridades competentes deverão poder tomar decisões quanto à definição de prioridades no recurso às medidas e meios de supervisão à sua disposição de forma proporcionada. Tal implica que as autoridades competentes possam tomar decisões quanto a essa definição de prioridades com base em metodologias de supervisão que deverão seguir uma abordagem baseada no risco. Mais especificamente, essas metodologias poderão compreender critérios ou parâmetros de referência para a classificação de entidades essenciais em categorias de risco e as correspondentes ações e meios de supervisão recomendados por categoria de risco, tais como a realização, a frequência ou o tipo de inspeções no local, as auditorias de segurança específicas ou as verificações de segurança, o tipo de informações a solicitar e o nível de pormenor dessas informações. Estas metodologias de supervisão podem também ser acompanhadas de programas de trabalho e ser avaliadas e revistas regularmente, nomeadamente quanto a aspetos como a afetação de recursos e as necessidades.

(70-AA) Em relação às entidades da administração pública, as competências de supervisão deverão ser exercidas em conformidade com os quadros e a ordem jurídica nacionais. Os Estados-Membros deverão poder decidir sobre a imposição de medidas de supervisão e execução adequadas, proporcionadas e eficazes em relação a essas entidades.

(70-AAA) A fim de demonstrar o cumprimento de determinadas medidas de gestão dos riscos de cibersegurança, os Estados-Membros poderão exigir que as entidades essenciais e importantes recorram a serviços de confiança qualificados ou sistemas de identificação eletrónica notificados nos termos do Regulamento (UE) n.º 910/2014.

(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.

(71-A) As disposições relativas à responsabilidade das pessoas singulares com certas responsabilidades no seio de uma entidade por incumprimento do seu dever de assegurar o cumprimento das obrigações estabelecidas na presente diretiva não exigem que os Estados-Membros assegurem a instauração de ação penal ou a constituição de responsabilidade civil por danos causados por tal incumprimento a terceiros.

(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 [...] **podem** 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.

(76-AA) A fim de assegurar uma supervisão e execução eficazes, nomeadamente nos casos com uma dimensão transfronteiriça, os Estados-Membros que tenham recebido um pedido de assistência mútua deverão, na medida do pedido, tomar medidas de supervisão e execução adequadas em relação à entidade que presta serviços ou que tem a rede e o sistema de informação no seu território.

(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) Deverá ser introduzido um [...] **sistema de** [...] **aprendizagem entre pares para ajudar a reforçar a** confiança **mútua e para se aprender com as boas práticas e experiências**, permitindo [...] **intercâmbios entre** peritos nomeados pelos Estados-Membros **sobre**[...] a execução das políticas de cibersegurança[...]. **Ao aplicar o sistema de aprendizagem entre pares, deverá ser dada especial atenção a que este não represente um encargo desnecessário ou desproporcionado para as autoridades competentes dos Estados-Membros. A Comissão deverá explorar todas as possibilidades de garantir potencialmente a cobertura financeira dos custos que possam resultar da organização de missões de aprendizagem entre pares. Além disso, o sistema de aprendizagem entre pares deverá ter em conta os resultados de mecanismos semelhantes, como o sistema de avaliação pelos pares da rede de CSIRT, acrescentar valor e evitar duplicações. A aplicação do sistema de aprendizagem entre pares não deverá prejudicar a legislação nacional ou da União em matéria de proteção de informações confidenciais e classificadas. Antes do início das rondas de aprendizagem entre pares, os Estados-Membros podem proceder a uma autoavaliação dos aspetos relevantes. A pedido do grupo de cooperação, a ENISA pode fornecer orientações para a autoavaliação e os modelos pertinentes, se for necessário. Os Estados-Membros poderão decidir publicar os respetivos relatórios.**

(80) [...]

(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**, às categorias de entidades a que deverá ser exigida a utilização de certos produtos, serviços e processos de TIC certificados**, é necessário atribuir competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[26].

(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.

[26] 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).

(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, **a fim de melhorar o funcionamento do mercado interno**.

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 mencionadas [...] nos anexos **I e II**[...];

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

Artigo 2.º

Âmbito

1. A presente diretiva aplica-se às entidades públicas e privadas **enumeradas** [...] nos [...] anexos I e II [...] **que cumpram ou excedam os limites máximos para médias empresas** [...] na aceção da Recomendação 2003/361/CE da Comissão[27]. **O artigo 3.º, n.º 4, o artigo 6.º, n.º 2, segundo e terceiro parágrafos, do anexo da referida recomendação não são aplicáveis para efeitos da presente diretiva.**

2. [...] **I**ndependentemente da [...] dimensão **das entidades referidas no n.º 1**, a presente diretiva também se aplica **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 qualificados de serviços de confiança referidos no anexo I, ponto XX,**

      iii) **prestadores não qualificados de serviços de confiança referidos no anexo I, ponto XX,**

      iv) registos de nomes de domínio de topo [...] referidos no anexo I, ponto 8,

   b) [...]

---

27 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).

c) A entidade é o único prestador, **num Estado-Membro**, de um serviço [...] **que é essencial para a manutenção de atividades societais ou económicas críticas**;

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

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

f) [...];

g) A entidade tenha sido identificada como entidade crítica nos termos da Diretiva (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[28] [Diretiva Resiliência das Entidades Críticas], **[**ou como uma entidade equivalente a uma entidade crítica nos termos do artigo 7.º da referida diretiva**]**.

2-A. A presente diretiva aplica-se igualmente às entidades da administração pública das administrações centrais, independentemente da sua dimensão, reconhecidas como tal num Estado-Membro, em conformidade com o direito nacional e referidas no ponto 9 do anexo I. Os Estados-Membros podem estabelecer que a presente diretiva se aplique igualmente às entidades da administração pública a nível regional e local.

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

3. [...]

A presente diretiva não prejudica as responsabilidades dos Estados-Membros de salvaguardar a segurança nacional ou o seu poder de salvaguardar outras funções fundamentais do Estado, incluindo a garantia da integridade territorial do Estado e a manutenção da ordem pública.

3-A. (1) A presente diretiva não se aplica:

a) às entidades não abrangidas pelo âmbito de aplicação do direito da União e, em qualquer caso, a nenhuma das entidades que exerçam principalmente atividades nos domínios da defesa, da segurança nacional, da segurança pública ou da aplicação da lei, independentemente da entidade que exerça tais atividades e do facto de ser uma entidade pública ou privada, sem prejuízo do ponto (2);

b) às entidades que exerçam atividades nos domínios judicial, dos parlamentos ou dos bancos centrais. [...]

(2) Sempre que as entidades da administração pública exerçam atividades nestes domínios apenas no quadro das suas atividades globais, devem ser excluídas na íntegra do âmbito de aplicação da presente diretiva.

3-AA. A presente diretiva não se aplica:

i) às atividades das entidades não abrangidas pelo âmbito de aplicação do direito da União e, em qualquer caso, a nenhuma das atividades relacionadas com a segurança nacional ou a defesa, independentemente da entidade que exerça tais atividades e do facto de ser uma entidade pública ou privada;

ii) às atividades das entidades do sistema judicial, dos parlamentos, dos bancos centrais e no domínio da segurança pública, incluindo entidades da administração pública que exerçam atividades de aplicação da lei para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou de execução de sanções penais.

3-AAA. As obrigações previstas na presente diretiva não implicam o fornecimento de informações cuja divulgação seja contrária aos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa.

3-AAAA. A presente diretiva não prejudica o direito da União em matéria de proteção de dados pessoais, nomeadamente o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE.

3-B. A presente diretiva não se aplica às entidades isentas do Regulamento (UE) XXXX/XXXX do Parlamento Europeu e do Conselho [Regulamento DORA], em conformidade com o artigo 2.º, n.º 4, do Regulamento DORA.

4. A presente diretiva é aplicável sem prejuízo [...][29] das Diretivas 2011/93/UE[30] e 2013/40/UE[31] 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 termos da presente diretiva**, 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.

---

29 [...]

30 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).

31 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).

Artigo 2.º-Bis

Entidades essenciais e importantes

1. Das entidades a que se aplica a presente diretiva, consideram-se essenciais:

i) as entidades previstas nos pontos 1 a 8-A e 10 do anexo I da presente diretiva que excedam os limites máximos para as médias empresas, na aceção da Recomendação 2003/361/CE da Comissão;

ii) as entidades de média dimensão a que se refere o artigo 2.º, n.º 2, alínea a), subalínea i);

iii) as entidades a que se refere o artigo 2.º, n.º 2, alínea a), subalíneas ii) e iv), da presente diretiva, independentemente da sua dimensão;

iv) as entidades a que se refere o artigo 2.º, n.º 2, alínea g), e artigo 2.º, n.º 2-A da presente diretiva, independentemente da sua dimensão;

v) se os Estados-Membros assim o estabelecerem, as entidades que os Estados-Membros tenham identificado, antes da entrada em vigor da presente diretiva, como operadores de serviços essenciais nos termos da Diretiva (UE) 2016/1148 ou do direito nacional;

vi) as entidades que excedam os limites máximos para as médias empresas, tal como definidos na Recomendação 2003/361/CE da Comissão, previstas no anexo II e que os Estados-Membros determinem que são essenciais com base nos critérios a que se refere o artigo 2.º, n.º 2, alíneas c) a e);

vii) as entidades de média dimensão, na aceção da Recomendação 2003/361/CE da Comissão, que os Estados-Membros determinem que são essenciais com base nos critérios a que se refere o artigo 2.º, n.º 2, alíneas c) a e);

viii) as micro ou pequenas entidades na aceção da Recomendação 2003/361/CE da Comissão previstas no n.º 2, alínea a), subalínea i), ou identificadas nos termos do n.º 2, alíneas c) a e), do presente artigo, que os Estados-Membros determinem que são essenciais com base nas avaliações de risco nacionais.

2. Das entidades a que se aplica a presente diretiva, consideram-se importantes:

i) as entidades previstas no anexo I da presente diretiva que possam ser consideradas médias empresas na aceção da Recomendação 2003/361/CE da Comissão e as entidades previstas no anexo II que cumpram ou excedam os limites máximos aplicáveis às médias empresas na aceção da Recomendação 2003/361/CE da Comissão[32];

ii) as entidades a que se refere o artigo 2.º, n.º 2, subalínea iii), da presente diretiva, independentemente da sua dimensão;

iii) as pequenas e microentidades a que se refere o artigo 2.º, n.º 2, alínea a), subalínea i);

iv) as pequenas e microentidades que os Estados-Membros determinem que são entidades importantes com base no artigo 2.º, n.º 2, alíneas c) a e).

---

32 **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).**

Artigo 2.º-A

Mecanismos de notificação

1. **Os Estados-Membros podem estabelecer um mecanismo nacional de autonotificação que exija a todas as entidades abrangidas pelo âmbito de aplicação da presente diretiva que comuniquem pelo menos o seu nome, endereço, dados de contacto, o setor em que operam ou o tipo de serviço que prestam e, se for caso disso, a lista dos Estados-Membros em que prestam serviços abrangidos pela presente diretiva, às autoridades competentes nos termos da presente diretiva ou aos organismos designados para o efeito pelos Estados-Membros.**

2. Os Estados-Membros [...] comunicam à Comissão, **no que respeita às entidades que tenham identificado nos termos do artigo 2.º, n.º 2, alíneas b) a e), pelo menos as informações relevantes quanto ao número de entidades identificadas, ao setor a que pertencem ou o tipo de serviço que prestam, em conformidade com o anexo, e as disposições específicas do artigo 2.º, n.º 2, com base nas quais foram identificadas, até [12 meses após o prazo de transposição da presente diretiva].** Os Estados-Membros devem rever [...] **estas informações** [...] regularmente, pelo menos de dois em dois anos, e atualizá-las quando necessário.

Artigo 2.º-B

Atos setoriais da União

1. Nos casos em que [...] atos **jurídicos setoriais da União** [...] exijam que entidades essenciais ou importantes [...] adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes ou [...] ciberameaças **significativos**, e, se tais exigências forem, na prática, pelo menos equivalentes às obrigações estabelecidas na presente diretiva, as correspondentes disposições desta última, **incluindo as disposições em matéria de supervisão e execução coerciva estabelecidas no capítulo VI**, não se aplicam **a essas entidades**. **Se os atos jurídicos setoriais da União não abrangerem todas as entidades de um setor específico que se insira no âmbito de aplicação da presente diretiva, as disposições pertinentes da presente diretiva continuam a aplicar-se às entidades não abrangidas por tais disposições setoriais.**

2. Os requisitos a que se refere o n.º 1 do presente artigo são considerados de efeito equivalente às obrigações estabelecidas na presente diretiva, se o respetivo ato setorial específico da União previr o acesso imediato e, quando se justifique, automático e direto, às notificações de incidentes pelas autoridades competentes nos termos da presente diretiva ou das CSIRT designadas e se:

a) as medidas de gestão dos riscos de cibersegurança forem, pelo menos, de efeito equivalente às estabelecidas no artigo 18.º, n.ºs 1 e 2, da presente diretiva; ou

b) os requisitos de notificação de incidentes significativos forem, pelo menos, de efeito equivalente aos estabelecidos no artigo 20.º, n.ºs 1 a 6.

3. A Comissão revê periodicamente a aplicação dos requisitos de efeito equivalente previstos nos n.ºs 1 e 2 do presente artigo em relação às disposições setoriais dos atos jurídicos da União. A Comissão consulta o grupo de cooperação e a ENISA aquando da preparação dessas revisões periódicas.

Artigo 3.º

Harmonização mínima

Sem prejuízo de outras obrigações que lhes incumbem por força do direito da União, os Estados-Membros podem [...] adotar ou manter disposições que garantam um elevado nível de cibersegurança **nos domínios abrangidos pela presente diretiva**.

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;

   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 qualquer **evento** que **possa** pôr em causa **[...]** a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou **dos** serviços oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis por intermédio destes;

2-A) "Serviços de comunicações eletrónicas": serviços de comunicações [...] eletrónicas, na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972;

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 prevê a governação para alcançar objetivos estratégicos **no domínio da** [...] **cibersegurança** [...] nesse Estado-Membro;

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 [...] oferecidos por redes e sistemas de informação ou acessíveis por intermédio destes;

5-A) "Incidente de cibersegurança em grande escala": um incidente com um impacto significativo em, pelo menos, dois Estados-Membros ou em que as perturbações causadas excedam a capacidade de resposta de um Estado-Membro.

---

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).

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;

6-A) "Risco": a possibilidade de perda ou perturbação causada por um incidente, expressa como uma combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do referido incidente;

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

7-**A) "Ciberameaça significativa": uma ciberameaça que, com base nas suas características técnicas, possa ser considerada suscetível de ter um impacto grave na rede e nos sistemas de informação de uma entidade ou dos seus utilizadores, causando perdas materiais ou imateriais consideráveis;**

8) "Vulnerabilidade": um ponto fraco, uma suscetibilidade ou uma falha de um ativo TIC ou sistema [...] passível de ser explorada por uma ciberameaça;

8-A. "Quase incidente": um evento que poderia ter causado danos à rede e aos sistemas de informação de uma entidade ou dos seus utilizadores, mas que foi impedido de se materializar plenamente;

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];

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 **para** [...] **utilização de terceiros, exceto os servidores de nomes da zona raiz** [...];

[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 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).

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, **excluindo as situações em que os nomes de domínio de topo são utilizados por um registo apenas para uso próprio**;

15-A) "Entidades que prestam serviços de registo de nomes de domínio para o domínio de topo": registos de nomes de domínio de topo, agentes de registo do domínio de topo e agentes de agentes de registo, tais como revendedores e prestadores de serviços de proxy;

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];

16-A) "Serviços de confiança": serviços de confiança na aceção do artigo 3.º, ponto 16, do Regulamento (UE) n.º 910/2014;

[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).

16-B) "Prestador qualificado de serviços de confiança": prestador qualificado de serviços de confiança na aceção do artigo 3.º, ponto 20, do Regulamento (UE) n.º 910/2014;

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, **inclusive quando esses recursos estão distribuídos por várias localizações**;

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;

---

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 do Parlamento Europeu e do Conselho e o Regulamento (CE) n.º 2006/2004 do Parlamento Europeu e do Conselho ("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 conectem, 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, **reconhecida como tal num Estado--Membro, nos termos da legislação nacional,** [...] que cumpra os seguintes critérios:

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

b) É dotada de personalidade jurídica **ou está habilitada por lei a agir em nome de outra entidade 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.

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 [...] **prevista no anexo I e designada como "essencial" em conformidade com o artigo 2.º-Bis, n.º 1**;

26) "Entidade importante": uma entidade [...] **prevista nos anexos I e II e designada como "importante" em conformidade com o artigo 2.º-Bis, n.º 2**;

26-A) "Produto de TIC": um produto de TIC na aceção do artigo 2.º, ponto 12, do Regulamento (UE) n.º 2019/881;

26-AA) "Serviço de TIC": um serviço de TIC na aceção do artigo 2.º, ponto 13, do Regulamento (UE) n.º 2019/881;

26-AB) "Processo de TIC": um processo de TIC na aceção do artigo 2.º, ponto 14, do Regulamento (UE) n.º 2019/881;

26-AC) "Prestador de serviços geridos": qualquer entidade que preste serviços, tais como redes, aplicações, infraestruturas e segurança, através de uma gestão contínua e regular, apoio e administração ativa nas instalações dos clientes, no seu centro de dados de prestador de serviços geridos (alojamento) ou num centro de dados de terceiros.

26-AD) "Prestador de serviços de segurança geridos": qualquer entidade que preste serviços de monitorização e gestão externalizados de dispositivos e sistemas de segurança. Dos serviços habituais fazem parte a gestão das barreiras de segurança, da deteção de intrusões, da rede privada virtual, da deteção de vulnerabilidades e dos serviços antivírus.

Inclui-se igualmente a utilização de centros operacionais de segurança de elevada disponibilidade (a partir das suas próprias instalações ou das de outros fornecedores de centros de dados) para prestar serviços 24 horas por dia destinados a reduzir o número de pessoal de segurança operacional que uma empresa necessita de contratar, formar e manter para assegurar uma postura de segurança aceitável.

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) [...] 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 várias autoridades e intervenientes que participam na execução da estratégia [...];

   c) [...] **Orientações** para identificar ativos importantes e **avaliar** 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) [...]

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 **riscos de cibersegurança**, bem como riscos, ameaças e **incidentes não relacionados com a cibersegurança**, e do exercício de funções de supervisão**, consoante o que for adequado**;

f-A) Quadro estratégico para a coordenação e cooperação entre as autoridades competentes nos termos da presente diretiva e as autoridades competentes designadas em conformidade com a legislação setorial.

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 [...] na prestação dos seus serviços;

b) **Uma política** [...] relativa à inclusão e à especificação de requisitos em matéria de cibersegurança aplicáveis a produtos e serviço**s** de TIC nos procedimentos de contratação pública**, incluindo a certificação de cibersegurança**;

c) Uma política **em matéria de gestão das vulnerabilidades, que abranja a promoção e a facilitação da** [...] divulgação coordenada **voluntária** de vulnerabilidades na aceção do artigo 6.º, **n. 1**;

d) Uma política relacionada com a manutenção da disponibilidade geral, [...] da integridade **e da confidencialidade** do núcleo público da Internet aberta;

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

---

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

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;

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. **Ao fazê-lo**, os Estados-Membros podem excluir **elementos da estratégia relacionados com** [...] a segurança nacional.

4. Os Estados-Membros devem avaliar as suas estratégias nacionais de cibersegurança com regularidade e pelo menos de [...] **cinco em cinco** 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, **o potencial titular da vulnerabilidade** e o fabricante ou fornecedor de produtos de TIC ou prestador de serviços de TIC. **Qualquer pessoa singular ou coletiva pode comunicar à CSIRT designada, eventualmente de forma anónima, a vulnerabilidade a que se refere o artigo 4.º, n.º 8. A CSIRT designada assegura o seguimento diligente da notificação e a confidencialidade da identidade da pessoa que comunica a vulnerabilidade.** Nos casos em que a vulnerabilidade notificada [...] **possa eventualmente ter um impacto importante sobre entidades em mais do que um Estado-Membro**, a CSIRT designada por cada Estado-Membro em causa deve**, sempre que adequado**, cooperar com **outras CSIRT designadas n**a rede de CSIRT**.**

2. A ENISA deve criar e manter um registo europeu de vulnerabilidades**, em consulta com o grupo de cooperação**. 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, **a título voluntário, vulnerabilidades do conhecimento público** 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 **emitidas pelas autoridades nacionais competentes ou pelas CSIRT** destinadas aos utilizadores de produtos e serviços vulneráveis sobre formas de minimizar os riscos resultantes das vulnerabilidades divulgadas. **A ENISA deve assegurar que o registo europeu de vulnerabilidades utiliza infraestruturas de comunicação e informação seguras e resilientes.**

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 de **cibersegurança** 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. **Os Estados-Membros devem assegurar a coerência com os quadros existentes de gestão geral de crises.**

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 de cibersegurança, **incluindo a sua integração no quadro geral nacional de gestão de crises,** e canais de intercâmbio de informações;

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

   e) Partes [...] interessadas 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 [...] **informar** a Comissão **da** designação das autoridades competentes a que se refere o n.º 1 e apresentar **as informações pertinentes relacionadas com os requisitos do n.º 3 do presente artigo quanto a**os respetivos planos nacionais de resposta a crises e incidentes de cibersegurança [...] no prazo de três meses a contar da designação e da adoção desses planos. Os Estados-Membros podem excluir informações específicas [...], na medida [...] necessária para salvaguardar a sua segurança nacional**, segurança pública ou defesa**.

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. **No exercício destas funções, as CSIRT podem dar prioridade à prestação de serviços específicos às entidades, com base numa abordagem baseada no risco.**

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 **aprendizagens** entre 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 [...] **canais de comunicação**, 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 **às autoridades competentes e** a outras partes interessadas, sobre ciberameaças, vulnerabilidades e incidentes;

c) Intervir em caso de incidentes;

d) Recolher e analisar dados forenses, proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança;

e) **[...]** Realizar uma análise proativa da rede e dos sistemas de informação [...] **para detetar vulnerabilidades com um potencial impacto importante, desde que, nos casos em que não houver autorização dessa entidade, a rede e os sistemas de informação não tenham sido sujeitos a intrusões nem o seu funcionamento tenha sido negativamente afetado;**

f) Participar na rede de CSIRT e prestar assistência mútua, **em conformidade com as suas capacidades e competências,** a outros membros da rede, a pedido destes.

f-A) Se for caso disso, atuar como coordenador para efeitos do processo de divulgação coordenada de vulnerabilidades nos termos do artigo 6.º, n.º 1, que deve incluir, em especial, a facilitação da interação entre as entidades notificadoras, o potencial titular da vulnerabilidade e o fabricante ou fornecedor de produtos de TIC ou serviços de TIC nos casos em que tal seja necessário, identificando e contactando as entidades em causa, apoiando as entidades notificadoras, negociando prazos de divulgação e gerindo vulnerabilidades que afetem várias organizações (divulgação coordenada de vulnerabilidades a várias partes).

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

3-A. As CSIRT podem estabelecer relações de cooperação com as CSIRT nacionais de países terceiros. No âmbito desta cooperação, podem trocar informações relevantes, incluindo dados pessoais, em conformidade com a legislação da União em matéria de proteção de dados.

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, **as CSIRT**, os pontos de contacto únicos e as autoridades policiais, as autoridades de proteção de dados e as autoridades **competentes designadas** [...] nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas[...]], **as autoridades competentes nos termos do Regulamento de Execução 2019/1583 da Comissão, as autoridades reguladoras nacionais designadas em conformidade com a Diretiva (UE) 2018/1972, as autoridades nacionais designadas nos termos do artigo 17.º do Regulamento (UE) n.º 910/2014,** [...] as autoridades financeiras designadas em conformidade com o Regulamento (UE) XXXX/XXXX do Parlamento Europeu e do Conselho [Regulamento DORA]**, bem como as autoridades competentes designadas por outros atos jurídicos setoriais da União** em cada Estado-Membro.

5. Os Estados-Membros devem garantir que as respetivas autoridades competentes **nos termos da presente diretiva e as autoridades competentes designadas em conformidade com a Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] trocam** regularmente [...] informações [...] sobre **a identificação de entidades críticas**, riscos de cibersegurança, ciber**ameaças e incidentes, bem como riscos; ameaças e incidentes não relacionados com a cibersegurança** 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 [...] em resposta a esses riscos e incidentes. **Os Estados-Membros devem garantir que as autoridades competentes nos termos da presente diretiva** [...] **e as autoridades competentes, designadas nos termos do Regulamento XXXX/XXXX [Regulamento DORA], a Diretiva 2018/1972 e o Regulamento (UE) 910/2014, trocam regularmente informações relevantes.**

No que diz respeito aos prestadores de serviços de confiança e, [...] em especial, nos casos em que essa função de supervisão nos termos da presente diretiva é atribuída a um organismo diferente das entidades supervisoras designadas nos termos do Regulamento (UE) n.º 910/2014, as autoridades nacionais competentes nos termos da presente diretiva devem cooperar estreitamente, em tempo útil, através do intercâmbio das informações relevantes, a fim de assegurar uma supervisão eficaz e o cumprimento pelos prestadores de serviços de confiança dos requisitos estabelecidos na presente diretiva e no Regulamento [XXXX/XXXX] **e, se for caso disso, a autoridade nacional competente nos termos da presente diretiva deverá informar, sem demora indevida, a entidade supervisora do eIDAS de qualquer ameaça ou incidente cibernético significativo notificado com impacto nos serviços de confiança**.

5-A. Com o objetivo [...] de simplificar a notificação de incidentes, os Estados-Membros podem estabelecer um ponto de entrada único para todas as notificações exigidas pela presente diretiva e também pelo Regulamento (UE) 2016/679 e pela Diretiva 2002/58/CE, quando tal se justifique. Os Estados-Membros podem recorrer ao ponto de entrada único para as notificações exigidas por outros atos jurídicos setoriais da União. Este ponto de entrada único não afeta a aplicação das disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE, em especial as relativas às autoridades de supervisão independentes.

CAPÍTULO III

*Cooperação **a nível da UE***

Artigo 12.º

Grupo de coordenação

1. É criado um grupo de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros, **bem como** [...] **para reforçar a confiança** [...].

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) **e as autoridades competentes designadas nos termos do Regulamento (UE) XXXX/XXXX [Regulamento DORA]**,[...] podem participar nas atividades do grupo de cooperação **em conformidade com o artigo 42.º, n.º 1, do Regulamento (UE) XXXX/XXXX [Regulamento DORA]**.

   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**;**

   a-A) Fornecer orientações para a elaboração e a execução de políticas em matéria de divulgação coordenada de vulnerabilidades, tal como se refere no artigo 5.º, n.º 2, alínea c),e no artigo 6.º, n.º 1;

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 [...] 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;

e-A) Trocar pontos de vista sobre a aplicação da legislação setorial que apresente aspetos de cibersegurança;

f) Discutir os relatórios das **aprendizagens entre** [...] pares a que se refere o artigo 16.º, n.º 7;

g) Discutir as **experiências recolhidas** [...] das atividades conjuntas de supervisão em casos transfronteiriços, tal como referido no artigo 34.º;

h) Fornecer orientações estratégicas à rede de CSIRT **e à Rede de Organizações de Coordenação de Cibercrises (EU–CyCLONe)** sobre questões emergentes específicas;

h-A) Trocar pontos de vista sobre o seguimento estratégico de incidentes de cibersegurança em grande escala com base nos ensinamentos retirados da rede de CSIRT e da EU-CyCLONe;

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**;**

k-A) Estabelecer o mecanismo de aprendizagem entre pares, em conformidade com o artigo 16.º da presente diretiva.

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 a **facilitar** 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, **designadas em conformidade com o artigo 9.º**, 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;

b-A) Proceder ao intercâmbio de informações sobre publicações e recomendações em matéria de cibersegurança;

b-B) Partilhar soluções técnicas que facilitem o tratamento técnico de incidentes;

b-C) Proceder ao intercâmbio de boas práticas, ferramentas e processos no que diz respeito às funções das CSIRT;

c) A pedido de um [...] **membro** 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 [...] **membro** 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, **proceder ao intercâmbio de boas práticas** 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, **a pedido de um Estado-Membro**;

h) Informar o grupo de cooperação sobre as suas atividades e sobre as outras formas de cooperação operacional discutidas nos termos da alínea g) **e** 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 **aprendizagens entre** [...] 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 **aprendizagens entre** [...] 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.

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

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 **ciber**crises dos Estados-Membros designadas nos termos do artigo 7.º [...]. **A Comissão participa nas atividades da rede na qualidade de observadora.** A ENISA assegura os serviços de secretariado da rede e presta apoio ao intercâmbio seguro de informações **e fornece os instrumentos necessários para apoiar a cooperação entre os Estados-Membros, garantindo o intercâmbio seguro de informações.**

Se for caso disso, a UE-CyCLONe pode convidar representantes de partes interessadas relevantes para participar nos seus trabalhos.

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

a) Aumentar o nível de preparação para a gestão de incidentes e crises de cibersegu[...]**ra**nça em grande escala;

b) Desenvolver um conhecimento situacional comum [...] sobre incidentes e crises de cibersegu**r**an[...]ça em grande escala;

b-A) Avaliar as consequências e o impacto de incidentes relevantes de cibersegurança em grande escala e propor eventuais medidas de atenuação;

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

d) **A pedido de um Estado-Membro**, discutir os **respetivos** planos nacionais de resposta a **crises** e incidentes de cibersegurança a que se refere o artigo 7.º, n.º **3** [...]**;**[...]

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

5. A UE-CyCLONe presta regularmente informações ao grupo de cooperação sobre **a gestão de incidentes de cibersegurança em grande escala e gestão de crises** [...], 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.

7. A EU-CyCLONe apresenta ao Parlamento Europeu e ao Conselho um relatório de avaliação dos seus trabalhos até [24 meses após a data de entrada em vigor da presente diretiva].

Artigo 14.º-A

Cooperação internacional

Quando adequado, a União pode 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, da rede de CSIRT e da EU-CyCLONe, em conformidade com a legislação da União em matéria de proteção de dados.

Artigo 15.º

Relatório sobre o estado da cibersegurança na União

1. A ENISA deve elaborar, em cooperação com a Comissão **e o grupo de cooperação**, um relatório bienal sobre o estado da cibersegurança na União. **Em especial**, [...] **e**ste relatório deve [...] incluir [...] os seguintes aspetos:

   a-A) Uma avaliação dos riscos de cibersegurança a nível da União, tendo em conta o panorama das ameaças;

   a) **Uma avaliação do** desenvolvimento das capacidades de cibersegurança nos setore**s** público e privado em toda a União;

   b) [...]

   c) **Uma avaliação agregada baseada em indicadores quantitativos e qualitativos** de cibersegurança [...] que contemple uma [...] **panorâmica** do nível de maturidade das capacidades de cibersegurança, **incluindo capacidades setoriais específicas**.

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

Aprendizagem entre pares

1. **Com vista a reforçar a confiança mútua, a alcançar um elevado nível comum de cibersegurança e a reforçar as capacidades e políticas de cibersegurança dos Estados-Membros necessárias para a eficácia da aplicação da presente diretiva,** [...] **o grupo de cooperação** [...] estabelece, **com o apoio da Comissão e** após consulta [...] à ENISA, **e, sempre que for relevante, a rede de CSIRT,** o mais tardar **24 [...]** meses após a entrada em vigor da presente diretiva, a metodologia [...] **de um sistema de aprendizagens [...] entre pares [...] objetivo, não discriminatório e justo relacionado** com a **aplicação da presente diretiva** pelos [...] Estados-Membros. **A participação na aprendizagem entre pares é voluntária.** O **sistema consiste em rondas de avaliações** [...] realizadas por peritos em cibersegurança [...] provenientes dos Estados-Membros [...] e deve incidir **sobre um ou mais dos** seguintes aspetos:

   i) a [...] 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) as [...] capacidades, incluindo os recursos [...] disponíveis, e o [...] desempenho das funções das autoridades nacionais competentes **a que se refere o artigo 8.º e as CSIRT a que se refere o artigo 9.º**,

[...]

ii[...])a [...] **implementação** da assistência mútua a que se refere o artigo 34.º,

iv) a [...] **aplicação** do quadro de partilha de informações a que se refere o artigo 26.º [...].

2. **Os critérios com base nos quais os Estados-Membros devem designar os peritos elegíveis para participarem nas rondas de aprendizagens entre pares devem ser** [...] objetivos, não discriminatórios, equitativos e transparentes [...] e **devem ser incluídos na metodologia a que se refere o n.º 1**. A ENISA e a Comissão [...] **podem** designar peritos para participarem nas [...] **rondas de aprendizagens entre pares** na qualidade de observadores. [...]

3. [...].

3-A. Antes do início das rondas de aprendizagem entre pares, os Estados-Membros podem proceder a uma autoavaliação dos aspetos abrangidos por cada ronda específica de aprendizagem entre pares e fornecer essa autoavaliação aos peritos designados a que se refere o n.º 2.

4. As [...] **aprendizagens** [...] entre pares **podem** incluir visitas virtuais ou **físicas** aos locais e discussões fora do local. Tendo em conta o princípio da boa cooperação, os Estados-Membros [...] **que participem na aprendizagem entre pares** devem facultar aos peritos designados as [...] informações solicitadas que sejam necessárias para a avaliação [...], **sem prejuízo da legislação nacional ou da União relacionadas com a proteção de informações confidenciais ou classificadas ou da salvaguarda de funções essenciais do Estado, como as que se enquadram no domínio da segurança nacional.** As informações obtidas durante o processo de **aprendizagem** entre [...] pares devem ser utilizadas exclusivamente para esse fim. Os peritos que participam na **aprendizagem** entre [...] pares não podem divulgar a terceiros quaisquer informações sensíveis ou confidenciais obtidas [...] **nesse contexto**. **O Estado-Membro que participa na aprendizagem entre pares pode opor-se à designação de determinados peritos por motivos devidamente justificados comunicados ao grupo de cooperação.**

5. Os aspetos que tenham sido objeto de uma ronda de aprendizagem entre pares [...] não serão objeto de novas rondas [...] de aprendizagens entre pares [...] para os Estado**s**-Membro**s** **participantes** nos [...] **quatro** anos seguintes à conclusão **dessa** [...] **ronda de aprendizagem** entre [...] pares, **salvo se o Estado-Membro em causa o solicitar ou concordar com uma proposta** do grupo de cooperação.

6. [...]

7. Os peritos que participam nas **rondas de aprendizagens** entre [...] pares devem elaborar relatórios sobre as constatações e conclusões dessas [...] **avaliações**. **Os Estados-Membros são autorizados a apresentar observações sobre os respetivos projetos de relatório, que devem ser anexadas ao relatório.** Os relatórios **finais** devem ser apresentados [...] ao grupo de cooperação [...]**, podendo os Estados-Membros decidir publicar os respetivos relatórios**.

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 [...] **podem ser** responsabilizados em caso de incumprimento das obrigações estabelecidas no referido artigo por parte das referidas entidades.

   A aplicação do presente número não prejudica a legislação nacional do Estado-Membro no que respeita às regras em matéria de responsabilidade nas instituições públicas, bem como à responsabilidade dos funcionários públicos e dos funcionários eleitos e nomeados.

2. Compete igualmente aos Estados-Membros **garantir que os membros do órgão de direção**[...] **são obrigados a** frequentar 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-**A. A presente diretiva aplica uma abordagem que contempla todos os riscos e inclui a proteção das redes, dos sistemas de informação e do seu ambiente físico contra qualquer evento suscetível de comprometer a disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados ou dos serviços oferecidos pelas redes e sistemas de informação ou acessíveis através destes.**

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 **e os custos da sua aplicação**. **Ao avaliar a proporcionalidade dessas medidas, devem ser tidos em devida conta o grau de exposição da entidade aos riscos, a sua dimensão, a probabilidade de ocorrência de incidentes e a sua gravidade. Tendo em consideração o nível e o tipo de risco para a sociedade em caso de incidentes que afetem entidades essenciais ou importantes, as medidas de gestão dos riscos de cibersegurança impostas às entidades importantes podem ser menos rigorosas do que as impostas às entidades essenciais.**

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, [...] resposta **e recuperação**[...] de 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 **diretos**, 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 [...] para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;

g) A **política seguida em matéria de** utilização de criptografia e cifragem;

g-A) A segurança dos recursos humanos, as políticas seguidas em matéria de controlo do acesso e a gestão de ativos.

3. Os Estados-Membros devem garantir que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), as entidades [...] **são obrigadas a** ter em conta as vulnerabilidades específicas de cada fornecedor **direto** 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. **Os Estados--Membros asseguram igualmente que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), as entidades são obrigadas a ter em conta os resultados das avaliações coordenadas dos riscos realizadas nos termos do artigo 19.º, n.º 1.**

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 **bem como, se necessário, as especificidades setoriais** dos elementos a que se refere o n.º 2 **do presente artigo**. **A Comissão adota, até [18 meses após a entrada em vigor da presente diretiva], atos de execução a fim de estabelecer as especificações técnicas e metodológicas para as entidades a que se refere o artigo 24.º, n.º 1, e para os prestadores de serviços de confiança a que se refere o ponto 8 do anexo I. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2.** Ao [...] preparar [...] **esses atos de execução**, a Comissão **segue**, na medida do possível, as normas internacionais e europeias, bem como as especificações técnicas pertinentes **e procede ao intercâmbio de pareceres com o grupo de cooperação e a ENISA sobre o projeto de ato de execução, em conformidade com o artigo 12.º, n.º 4, alínea d).**

6. [...]

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, **dos** 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. **O ato de notificação em si não acarreta responsabilidades acrescidas para a entidade notificadora.**

2. [...]

Quando for o caso, [...] **as entidades essenciais e importantes** 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. O **ato de** notificação **em si** 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 **do serviço** ou perdas financeiras **graves** [...] 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, **na forma de um alerta rápido**, 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 inicial** 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). **Em especial, pode justificar-se o não cumprimento do prazo referido na alínea c) nos casos em que o incidente ainda esteja em curso.**

5. 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, [...] **sem demora justificada,** 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, a CSIRT ou **o ponto de contacto único** devem informar os outros Estados-Membros afetados e a ENISA do incidente. **Essas informações devem incluir, pelo menos, os elementos previstos no n.º 4 do presente artigo.** 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 do número[...] 1 [...] aos pontos de contacto únicos dos outros Estados-Membros afetados.

9. O ponto de contacto único deve apresentar [...] **semestralmente** 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 do número[...] 1 [...] 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. **A ENISA informa semestralmente o grupo de cooperação e a rede de CSIRT das suas conclusões das notificações recebidas.**

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. Os referidos 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 utilizem determinados produtos,** [...] **serviços e** [...] **processos de TIC certificados** no âmbito de sistemas europeus de certificação da cibersegurança específicos adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881. Os produtos **de TIC**, serviços e processos sujeitos a certificação podem ser desenvolvidos por uma entidade essencial ou importante ou ser adquiridos a terceiros.

2. A Comissão pode [...] adotar [...] atos de **execução** que especifiquem as categorias de entidades essenciais **ou importantes** obrigadas **a utilizar determinados produtos, serviços e processos de TIC certificados ou a** obter um certificado [...] no âmbito de [...] sistemas europeus de certificação da cibersegurança **adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881.**[...] **Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2. Ao preparar esses atos de execução, a Comissão deve, em conformidade com o artigo 56.º do Regulamento (UE) 2019/881:**

   i) Tomar em consideração o impacto das medidas para os fabricantes de produtos, os prestadores de serviços e os fornecedores de processos de TIC e para os utilizadores em termos de custos dessas medidas, os benefícios societais ou económicos decorrentes do reforço previsto do nível de segurança para os produtos, serviços e processos de TIC visados, assim como a sua disponibilidade alternativa no mercado;

   ii) Proceder a uma consulta aberta, transparente e inclusiva de todas as partes interessadas e Estados-Membros;

(iii) Tomar em consideração os prazos de aplicação, as medidas e os períodos de transição, tendo especialmente em conta o eventual impacto das medidas para os fabricantes de produtos ou prestadores de serviços ou processos de TIC, bem como para os utilizadores, incluindo as PME;

(iv) Ter em conta a existência e a aplicação da legislação pertinente dos Estados-Membros.

3. A Comissão pode solicitar à ENISA a elaboração de um projeto de sistema **ou a revisão de um sistema europeu de certificação da cibersegurança existente** 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 **do presente artigo**.

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 nome** 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**, incluindo, pelo menos, os seguintes dados:**

   a) Nome de domínio

   b) Data de registo

   c) Dados do requerente de registo, incluindo:

      i) no caso das pessoas singulares – nome, apelido e endereço eletrónico;

      ii) no caso das pessoas coletivas – nome e endereço eletrónico.

3. Os Estados-Membros devem ainda garantir que os registos **de nome** 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 nome** 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 nome** 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 nome** 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 **e, em qualquer caso, no prazo de 72 horas**. 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-A. Considera-se que as entidades abrangidas pela presente diretiva estão sob a jurisdição do Estado-Membro onde prestam os seus serviços. Considera-se que as entidades referidas nos pontos 1 a 7 e 10 do anexo I, os prestadores de serviços de confiança e os fornecedores de pontos de troca de tráfego referidos no ponto 8 do anexo I e nos pontos 1 a 5 do anexo II estão sob a jurisdição do Estado-Membro em cujo território tais entidades se encontram estabelecidas.

1. Considera-se que os prestadores de serviços de DNS, os registos de nomes de domínio de topo[...]**, as entidades que prestam serviços de registo de nomes de domínio a esses registos**, os prestadores de serviços de computação em nuvem, os prestadores de serviços de centro de dados [...] os fornecedores de redes de distribuição de conteúdos**, os prestadores de serviços geridos e os prestadores de serviços de segurança geridos** referidos no anexo I, ponto 8 **e ponto 8-A**, 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 **predominantemente** tomadas as decisões relacionadas com as medidas de gestão dos riscos de cibersegurança. Se **o local onde tais decisões são predominantemente tomadas não puder ser determinado ou 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. **Se os serviços forem prestados por um grupo de empresas, deve considerar-se que o seu estabelecimento principal é o estabelecimento principal do grupo.**

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.

4-A. Os Estados-Membros que tenham recebido um pedido de assistência mútua em relação às entidades referidas no n.º 1 podem, dentro dos limites do pedido, tomar medidas de supervisão e execução adequadas em relação à entidade que presta serviços ou que tem a rede e o sistema de informação no seu território.

Artigo 25.º

Registo de determinadas entidades de infraestruturas digitais e de prestadores de serviços digitais

1. [...] **Os Estados-Membros asseguram que** as entidades **a que se refere o artigo 24.º, n.º 1, que tenham o seu estabelecimento principal no seu território ou, se não estiverem estabelecidas na União, tenham o seu representante designado na União estabelecido no seu território são obrigadas a** [...] apresentar as seguintes informações **às autoridades competentes** até [12 meses após a entrada em vigor da diretiva]:

a) Nome da entidade;

a-A) Tipo de entidade, em conformidade com os anexos I e II da presente diretiva;

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 **e dos seus representantes;**

d) Estados-Membros onde a entidade presta serviços.

Se for o caso, tais informações devem ser apresentadas por intermédio do mecanismo nacional[...] de autonotificação a que se refere o artigo 2.º-A.

2. **Os Estados-Membros devem assegurar que as**[...] entidades referidas no n.º 1 [...] **também comunicam** 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. [...] **Os pontos de contacto únicos dos Estados-Membros** devem comunicar [...] à [...] **ENISA as informações referidas nos n.ºs 1 e 2**. [...]

3-A. Com base nas informações que receber nos termos do n.º 3 do presente artigo, a ENISA cria e conserva um registo para as entidades referidas no n.º 1. A pedido dos Estados-Membros, a ENISA dá acesso ao registo às autoridades competentes relevantes, fornecendo simultaneamente as garantias necessárias para proteger a confidencialidade das informações, consoante o caso.

4. [...]

CAPÍTULO V

Partilha de informações

Artigo 26.º

Acordos de partilha de informações sobre cibersegurança

1. [...] Os Estados-Membros devem assegurar que as entidades essenciais e importantes podem proceder**, a título voluntário,** ao intercâmbio de informações pertinentes sobre cibersegurança, nomeadamente relacionadas com ciberameaças, **quase incidentes,** 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 entidades essenciais e importantes. Tal intercâmbio deve ser executado mediante acordos de partilha de informações que protejam a natureza potencialmente sensível das informações partilhadas [...].

3. Os Estados-Membros [...] **podem** 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 [...] **podem** 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. [...] 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

1. Sem prejuízo do disposto no artigo 20.º, os Estados-Membros devem assegurar que as entidades essenciais e importantes podem notificar, a título voluntário, as autoridades competentes ou as CSIRT de quaisquer incidentes, ciberameaças ou quase acidentes relevantes.

2. 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. **Sem prejuízo da investigação, deteção e repressão de infrações penais, 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.

3. As notificações voluntárias só são tratadas se esse tratamento não constituir um ónus desproporcionado ou indevido para os Estados-Membros em causa.

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**,** [...] 20.º **e 23.º**. **Os Estados-Membros podem autorizar as autoridades competentes a dar prioridade à supervisão, que deve orientar-se por uma abordagem baseada no risco.**

2. Quando tratarem de incidentes de cibersegurança, as autoridades competentes devem trabalhar em estreita colaboração com as autoridades encarregadas da proteção de dados, **as autoridades competentes designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas], os organismos de supervisão designados nos termos do Regulamento (UE) n.º 910/2014 e outras autoridades competentes designadas em conformidade com atos jurídicos setoriais da União**. [...]

3. Sem prejuízo dos quadros legislativos e institucionais nacionais, os Estados-Membros devem assegurar que, na supervisão do cumprimento da presente diretiva pelas entidades da administração pública e na execução coerciva de eventuais sanções em caso de incumprimento, as autoridades competentes disponham dos poderes adequados para desempenhar essas funções com independência operacional em relação às entidades supervisionadas. Os Estados-Membros podem decidir impor medidas de supervisão e execução coerciva adequadas, proporcionadas e eficazes em relação a essas entidades, em conformidade com os quadros e a ordem jurídica nacionais.

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 **seguem uma abordagem baseada no risco e** dispõem de poderes para submeter essas entidades **pelo menos** a:

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

   b) Auditorias **de segurança** 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**, sempre que necessários por razões técnicas, em cooperação com a entidade em causa**;

   e) Pedidos de informações necessárias para avaliar as medidas de cibersegurança adotadas pela entidade, incluindo políticas de cibersegurança documentadas [...];

   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.

2-A. No exercício das suas funções de supervisão previstas no n.º 2 do presente artigo, as autoridades competentes podem estabelecer metodologias de supervisão que permitam hierarquizar essas tarefas de acordo com uma abordagem baseada no risco.

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 **pelo menos**:

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**, da natureza da ameaça, bem como** 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) [...]

h) Ordenar que essas entidades tornem públicos os aspetos do não cumprimento das obrigações estabelecidas na presente diretiva de uma determinada forma**, quando essa divulgação pública não conduza a uma exposição prejudicial da respetiva entidade**;

i) [...]

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 **ou a tribunais competentes, de acordo com a legislação nacional** 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.

As sanções previstas no presente número não são aplicáveis às entidades da administração pública abrangidas pela presente diretiva.

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. **No que diz respeito às entidades da administração pública, a presente disposição não prejudica a legislação dos Estados-Membros em matéria de responsabilidade dos funcionários públicos e dos funcionários eleitos e nomeados.**

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**, exceto em caso de perigo iminente**.

9. Os Estados-Membros devem assegurar que as suas autoridades competentes **nos termos da presente diretiva** informam as autoridades competentes **no mesmo** [...] Estado-Membro [...] 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. **Consoante o caso,** [...] autoridades competentes ao abrigo da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas][...] **podem solicitar** às autoridades competentes **nos termos da presente diretiva** [...] que exerçam os seus **poderes** de supervisão e execução **em relação a** uma entidade essencial no âmbito da presente diretiva que seja igualmente identificada como crítica **[**ou equivalente**] nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas].**

10. Os Estados-Membros asseguram que as suas autoridades competentes nos termos da presente diretiva informam o Fórum de Fiscalização em conformidade com o artigo 29.º, n.º 1, do Regulamento (UE) XXXX/XXXX [DORA] no exercício dos seus poderes de supervisão e execução coerciva destinados a assegurar o cumprimento das obrigações decorrentes da presente diretiva por parte de uma entidade essencial designada como terceiro fornecedor de serviços TIC críticos nos termos do artigo 28.º do Regulamento (UE) XXXX/XXXX [DORA].

10-A. Os Estados-Membros asseguram que as suas autoridades competentes nos termos da presente diretiva informam as autoridades competentes relevantes designadas nos termos do Regulamento (UE) n.º 910/2014 no exercício dos seus poderes de supervisão e execução coerciva destinados a assegurar o cumprimento, por parte de uma entidade designada como prestadores de serviços de confiança nos termos do Regulamento (UE) n.º 910/2014, das obrigações decorrentes da presente diretiva.

Artigo 30.º

Supervisão e execução coerciva no respeitante a entidades importantes

1. Sempre que lhes sejam apresentadas provas, indícios **ou informações** de que uma entidade importante não está **alegadamente** 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 **seguem uma abordagem baseada no risco e** dispõem de poderes para submeter essas entidades **pelo menos** 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, **não discriminatórios**, equitativos e transparentes**, sempre que necessários por razões técnicas, em cooperação com a entidade em causa;**

   d) Pedidos de quaisquer informações necessárias para avaliar ex post as medidas de cibersegurança[...];

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

   e-A) 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.

2-A. No exercício das suas funções de supervisão previstas no n.º 2 do presente artigo, as autoridades competentes podem estabelecer metodologias de supervisão que permitam hierarquizar essas tarefas de acordo com uma abordagem baseada no risco.

3. Ao exercerem os poderes previstos no n.º 2, alíneas d) **a e-A)**, 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 **pelo menos**:

   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**, da natureza da ameaça, bem como** 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 obrigações estabelecidas na presente diretiva de uma determinada forma**, quando essa divulgação pública não conduza a uma exposição prejudicial da respetiva entidade**;

h) [...]

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 [...].

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 **cometidas pelas entidades essenciais** são sujeitas, nos termos dos n.ºs 2 e 3 do presente artigo, a coimas num montante máximo não inferior a **4**[...] 000 000 de euros ou**, no caso de uma pessoa coletiva,** [...] a 2 % do volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, da empresa a que a entidade essencial [...] pertence, consoante o montante que for mais elevado.

4-A. Os Estados-Membros devem assegurar que as violações das obrigações previstas nos artigos 18.º ou 20.º cometidas pelas entidades importantes são sujeitas, nos termos dos n.ºs 2 e 3 do presente artigo, a coimas num montante máximo não inferior a 2 000 000 de euros ou, no caso de uma pessoa coletiva, a 1 % do volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, da empresa a que a entidade 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.

6-A. Quando o sistema jurídico dos Estados-Membros não preveja coimas, o Estado-Membro deve garantir que o presente artigo pode ser aplicado de modo a que a coima seja proposta pela autoridade de controlo competente e imposta pelos tribunais nacionais competentes, garantindo ao mesmo tempo que estas medidas jurídicas corretivas são eficazes e têm um efeito equivalente às coimas impostas pelas autoridades de controlo. Em todo o caso, as coimas impostas devem ser efetivas, proporcionadas e dissuasivas. Os referidos Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do presente número até […] e, sem demora, de qualquer alteração subsequente das mesmas.

Artigo 32.º

Infrações que implicam uma violação de dados pessoais

1. Se, **durante uma ação de supervisão ou execução,** as autoridades competentes [...] **tomarem conhecimento** de que a infração das obrigações estabelecidas nos artigos 18.º e 20.º **da presente diretiva** por parte de uma entidade essencial ou importante pode implicar[...] 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**, sem demora injustificada,** informar as autoridades de controlo competentes nos termos dos artigos 55.º e 56.º do referido regulamento [...].

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 **a que se refere o artigo 8.º da presente diretiva** não podem aplicar [...] **uma** coima **por uma infração constituída pelos mesmos factos previstos**[...] no 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 [...] **prestar serviços** em **um ou mais** Estado**s**-Membro**s**, mas as suas redes e sistemas de informação estiverem situados noutro ou noutros Estados-Membros, as autoridades competente**s** dos Estado**s**-Membro**s em causa** [...] 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 [...];

b) Uma autoridade competente possa solicitar a outra autoridade competente que tome as medidas de supervisão ou coercivas [...];

c) Uma autoridade competente, ao receber um pedido justificado de outra autoridade competente, preste **à mesma** assistência**, proporcionada aos recursos de que dispõe,** para que as medidas de supervisão ou coercivas [...] 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, [...] se determine que [...] a autoridade não tem competência para prestar a assistência solicitada, **não dispõe dos recursos necessários** ou que a assistência solicitada não é proporcionada às funções de supervisão da autoridade competente desempenhadas [...] **ou se o pedido disser respeito a informações ou implicar atividades que sejam contrárias à segurança nacional, à segurança pública ou à defesa desse Estado-Membro**.

2. Quando adequado e de comum acordo, as autoridades competentes de diferentes Estados-Membros podem realizar as ações de supervisão conjuntas [...].

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 [...] **os** efeitos **de tal avaliação,** [...], a Comissão tem em conta os relatórios da [...] rede de CSIRT sobre a experiência adquirida a nível [...] operacional. O primeiro relatório deve ser apresentado até … [54 meses após a data de entrada em vigor da presente diretiva].

Artigo 36.º

[...]

[...]

[...]

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** … [[...] **24** 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

No Regulamento (UE) n.º 910/2014, o artigo 19.º [...] é suprimido **com efeitos a partir de... [data do prazo de transposição da presente diretiva].**

Artigo 40.º

Alteração da Diretiva (UE) 2018/1972

Na Diretiva (UE) 2018/1972, os artigos 40.º e 41.º [...] são suprimidos **com efeitos a partir de... [data do prazo de transposição da presente diretiva]**.

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 II[...].

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	*Pelo Conselho*
O Presidente	*O Presidente*

ANEXO I

SETORES, SUBSETORES E TIPOS DE ENTIDADES

Setor	Subsetor	Tipo de entidade
1. Energia	a) Eletricidade	— Empresas de eletricidade na aceção do artigo 2.º, ponto 57, da Diretiva (UE) 2019/944 que exercem a atividade de "comercialização" na aceção do artigo 2.º, ponto 12, da mesma diretiva ([39])
		— Operadores da rede de distribuição na aceção do artigo 2.º, ponto 29, da Diretiva (UE) 2019/944
		— Operadores da rede de transporte na aceção do artigo 2.º, ponto 35, da Diretiva (UE) 2019/944
		— Produtores na aceção do artigo 2.º, ponto 38, da Diretiva (UE) 2019/944
		— Operadores nomeados do mercado da eletricidade na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/943 ([40])
		— Participantes no mercado da eletricidade na aceção do artigo 2.º, ponto 25, do Regulamento (UE) 2019/943, que prestam serviços de agregação, resposta da procura ou armazenamento de energia na aceção do artigo 2.º, pontos 18, 20 e

[39] Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativa a regras comuns para o mercado interno da eletricidade e que altera a Diretiva 2012/27/UE (JO L 158 de 14.6.2019, p. 125).

[40] Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativo ao mercado interno da eletricidade (JO L 158 de 14.6.2019, p. 54).

		59, da Diretiva (UE) 2019/944
	b) Sistemas de aquecimento e arrefecimento urbano	— Sistemas de aquecimento ou arrefecimento urbano na aceção do artigo 2.º, ponto 19, da Diretiva (UE) 2018/2001 ([41]) relativa à promoção da utilização de energia de fontes renováveis
	c) Petróleo	— Operadores de oleodutos de petróleo
		— Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
		— Entidades centrais de armazenagem de petróleo na aceção do artigo 2.º, alínea f), da Diretiva 2009/119/CE do Conselho ([42])
	d) Gás	— Empresas de comercialização na aceção do artigo 2.º, ponto 8, da Diretiva 2009/73/CE ([43])
		— Operadores da rede de distribuição na aceção do artigo 2.º, ponto 6, da Diretiva 2009/73/CE
		— Operadores da rede de transporte na aceção do artigo 2.º, ponto 4, da Diretiva 2009/73/CE
		— Operadores do sistema de

41 Diretiva (UE) 2018/2001 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, relativa à promoção da utilização de energia de fontes renováveis (JO L 328 de 21.12.2018, p. 82).

42 Diretiva 2009/119/CE do Conselho, de 14 de setembro de 2009, que obriga os Estados-Membros a manterem um nível mínimo de reservas de petróleo bruto e/ou de produtos petrolíferos (JO L 265 de 9.10.2009, p. 9).

43 Diretiva 2009/73/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece regras comuns para o mercado interno do gás natural e que revoga a Diretiva 2003/55/CE (JO L 211 de 14.8.2009, p. 94).

		armazenamento na aceção do artigo 2.º, ponto 10, da Diretiva 2009/73/CE
		— Operadores da rede de GNL na aceção do artigo 2.º, ponto 12, da Diretiva 2009/73/CE
		— Empresas de gás natural na aceção do artigo 2.º, ponto 1, da Diretiva 2009/73/CE
		— Operadores de instalações de refinamento e tratamento de gás natural
	e) Hidrogénio	Operadores de produção, armazenamento e transporte de hidrogénio
2. Transportes	a) Transporte aéreo	— Transportadoras aéreas na aceção do artigo 3.º, ponto 4, do Regulamento (CE) n.º 300/2008 ([44]) **utilizadas para fins comerciais**
		— Entidades gestoras aeroportuárias na aceção do artigo 2.º, ponto 2, da Diretiva 2009/12/CE ([45]), aeroportos na aceção do artigo 2.º, ponto 1, da mesma diretiva, incluindo os aeroportos principais enumerados no anexo II, ponto 2, do Regulamento (UE) n.º 1315/2013 ([46]), e as entidades que exploram instalações anexas existentes dentro dos aeroportos

[44] Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

[45] Diretiva 2009/12/CE do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativa às taxas aeroportuárias (JO L 70 de 14.3.2009, p. 11).

[46] Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2013, relativo às orientações da União para o desenvolvimento da rede transeuropeia de transportes e que revoga a Decisão n.º 661/2010/UE (JO L 348 de 20.12.2013, p. 1).

		— Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo (CTA) na aceção do artigo 2.º, ponto 1, do Regulamento (CE) n.º 549/2004 ([47])
	b) Transporte ferroviário	— Gestores de infraestrutura na aceção do artigo 3.º, ponto 2, da Diretiva 2012/34/UE ([48])
		— Empresas ferroviárias na aceção do artigo 3.º, ponto 1, da Diretiva 2012/34/UE, incluindo os operadores de instalações de serviço na aceção do artigo 3.º, ponto 12, da Diretiva 2012/34/UE
	c) Transporte aquático	— Companhias de transporte marítimo, costeiro e por vias navegáveis interiores de passageiros e de mercadorias, na aceção, para o transporte marítimo, do anexo I do Regulamento (CE) n.º 725/2004 ([49]), não incluindo os navios explorados por essas companhias
		— Entidades gestoras de portos na aceção do artigo 3.º, ponto 1, da Diretiva 2005/65/CE ([50]), incluindo as respetivas instalações portuárias na aceção do artigo 2.º, ponto 11, do Regulamento (CE) n.º 725/2004, e as entidades que gerem as obras e o equipamento existente dentro dos portos

47 Regulamento (CE) n.º 549/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que estabelece o quadro para a realização do céu único europeu (Regulamento-Quadro) (JO L 96 de 31.3.2004, p. 1).

48 Diretiva 2012/34/UE do Parlamento Europeu e do Conselho, de 21 de novembro de 2012, que estabelece um espaço ferroviário europeu único (JO L 343 de 14.12.2012, p. 32).

49 Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, de 31 de março de 2004, relativo ao reforço da proteção dos navios e das instalações portuárias (JO L 129 de 29.4.2004, p. 6).

50 Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, de 26 de outubro de 2005, relativa ao reforço da segurança nos portos (JO L 310 de 25.11.2005, p. 28).

		— Operadores de serviços de tráfego marítimo na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE ([51])
	d) Transporte rodoviário	— Autoridades rodoviárias na aceção do artigo 2.º, ponto 12, do Regulamento Delegado (UE) 2015/962 da Comissão ([52]), responsáveis pelo controlo da gestão do tráfego**, com exceção das entidades públicas para as quais a gestão do tráfego ou os operadores de sistemas de transporte inteligentes constituem apenas uma parte não essencial da sua atividade geral**
		— Operadores de sistemas de transporte inteligentes na aceção do artigo 4.º, ponto 1, da Diretiva 2010/40/UE ([53])
3. Setor bancário		— Instituições de crédito na aceção do artigo 4.º, ponto 1, do Regulamento (UE) n.º 575/2013 ([54])**, [exceto as referidas no artigo 2.º, n.º 5, ponto 8, da Diretiva 2013/36/UE, que estão isentas nos termos do artigo 2.º, n.º 4, do Regulamento XX [DORA]]**

51 Diretiva 2002/59/CE do Parlamento Europeu e do Conselho, de 27 de junho de 2002, relativa à instituição de um sistema comunitário de acompanhamento e de informação do tráfego de navios e que revoga a Diretiva 93/75/CEE do Conselho (JO L 208 de 5.8.2002, p. 10).

52 Regulamento Delegado (UE) 2015/962 da Comissão, de 18 de dezembro de 2014, que complementa a Diretiva 2010/40/UE do Parlamento Europeu e do Conselho no respeitante à prestação de serviços de informação de tráfego em tempo real à escala da UE (JO L 157 de 23.6.2015, p. 21).

53 Diretiva 2010/40/UE do Parlamento Europeu e do Conselho, de 7 de julho de 2010, que estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte (JO L 207 de 6.8.2010, p. 1).

54 Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).

4. Infraestruturas do mercado financeiro		— Operadores de plataformas de negociação na aceção do artigo 4.º, ponto 24, da Diretiva 2014/65/UE ([55])
		— Contrapartes centrais (CCP) na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 648/2012 ([56])
5. Saúde		— Prestadores de cuidados de saúde na aceção do artigo 3.º, alínea g), da Diretiva 2011/24/UE ([57])
		— Laboratórios de referência da UE na aceção do artigo 15.º do Regulamento (UE) XXXX/XXXX relativo às ameaças transfronteiriças graves para a saúde[58]
		— Entidades que realizam atividades de investigação e desenvolvimento de medicamentos na aceção do artigo 1.º, ponto 2, da Diretiva 2001/83/CE ([59]) — Entidades que fabricam produtos farmacêuticos de base e preparações farmacêuticas referidas na secção C, divisão 21, da NACE Rev. 2 — Entidades que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde

55 Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173 de 12.6.2014, p. 349).

56 Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 201 de 27.7.2012, p. 1).

57 Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).

58 [Regulamento do Parlamento Europeu e do Conselho relativo às ameaças transfronteiriças graves para a saúde e que revoga a Decisão n.º 1082/2013/UE — referência a atualizar quando a proposta COM(2020) 727 final for adotada].

59 Diretiva 2001/83/CE do Parlamento Europeu e do Conselho, de 6 de novembro de 2001, que estabelece um código comunitário relativo aos medicamentos para uso humano (JO L 311 de 28.11.2001, p. 67).

		pública ("lista de dispositivos médicos críticos para a emergência de saúde pública") na aceção do artigo 20.º do Regulamento (UE) XXXX/XXXX[60]
6. Água potável		Fornecedores e distribuidores de água destinada ao consumo humano na aceção do artigo 2.º, ponto 1, alínea a), da Diretiva 98/83/CE do Conselho ([61]), mas excluindo os distribuidores para os quais a distribuição de água para consumo humano constitui apenas uma parte **não-essencial** da atividade geral de distribuição de outros produtos de base e mercadoria [...]
7. Águas residuais		Empresas que recolhem, eliminam ou tratam águas residuais urbanas, domésticas e industriais na aceção do artigo 2.º, pontos 1 a 3, da Diretiva 91/271/CEE do Conselho ([62]) **mas excluindo as empresas para as quais a recolha, eliminação ou tratamento de águas residuais urbanas, domésticas e industriais constitui apenas uma parte não essencial da sua atividade geral.** [...]
8. Infraestruturas digitais		**—** Fornecedores de pontos de troca de tráfego
		— Prestadores de serviços de DNS**, excluindo operadores de servidores de nomes da zona raiz**
		— Registos de nomes de domínio de topo
		— Prestadores de serviços de computação em nuvem

60 [Regulamento do Parlamento Europeu e do Conselho relativo ao reforço do papel da Agência Europeia de Medicamentos em matéria de preparação e gestão de crises no que diz respeito aos medicamentos e dispositivos médicos — referência a atualizar quando a proposta COM(2020) 725 final for adotada].

61 Diretiva 98/83/CE do Conselho, de 3 de novembro de 1998, relativa à qualidade da água destinada ao consumo humano (JO L 330 de 5.12.1998, p. 32).

62 Diretiva 91/271/CEE do Conselho, de 21 de maio de 1991, relativa ao tratamento de águas residuais urbanas (JO L 135 de 30.5.1991, p. 40).

		— Prestadores de serviços de centro de dados
		— Fornecedores de redes de distribuição de conteúdos
		— Prestadores de serviços de confiança na aceção do artigo 3.º, ponto 19, do Regulamento (UE) n.º 910/2014 (**63**)
		— Fornecedores de redes públicas de comunicações eletrónicas na aceção do artigo 2.º, ponto 8, da Diretiva (UE) 2018/1972 (**64**) ou prestadores de serviços de comunicações eletrónicas na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972, nos casos em que esses serviços estejam acessíveis ao público
8-A Gestão dos serviços das TIC **(B2B)**		**— Prestador de serviços geridos** **— Prestador de serviços de segurança geridos**
9. **Entidades** da administração pública		— Entidades da administração pública a nível central **tal como definidas pelos Estados-Membros em conformidade com a legislação nacional** — [...]**65**[...] — [...]

63 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).

64 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).

65 [...]

10. Espaço		— Operadores de infraestruturas terrestres, detidas, geridas e operadas por Estados-Membros ou entidades privadas, que apoiam a prestação de serviços espaciais, excluindo os fornecedores de redes públicas de comunicações eletrónicas na aceção do artigo 2.º, ponto 8, da Diretiva (UE) 2018/1972

ANEXO II

SETORES, SUBSETORES E TIPOS DE ENTIDADES

Setor	Subsetor	Tipo de entidade
1. Serviços postais e de estafeta		Prestadores de serviços postais na aceção do artigo 2.º, ponto 1[...], da Diretiva 97/67/CE ([66]) **incluindo** [...] prestadores de serviços de estafeta
2. Gestão de resíduos		Empresas que realizam a gestão de resíduos na aceção do artigo 3.º, ponto 9, da Diretiva 2008/98/CE ([67]), mas excluindo as empresas para as quais a gestão de resíduos não constitui a atividade económica principal

[66] 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)**, com a redação que lhe foi dada pela Diretiva 2008/6/CE do Parlamento Europeu e do Conselho, de 20 de fevereiro de 2008, que altera a Diretiva 97/67/CE no respeitante à plena realização do mercado interno dos serviços postais da Comunidade (JO L 52 de 27.2.2008, p. 3)**.

[67] Diretiva 2008/98/CE do Parlamento Europeu e do Conselho, de 19 de novembro de 2008, relativa aos resíduos e que revoga certas diretivas (JO L 312 de 22.11.2008, p. 3).

3. Produção, fabrico e distribuição de produtos químicos		Empresas que realizam a produção [...] e a distribuição de substâncias e de [...] **misturas** na aceção do artigo 3.º, pontos [...] 9 e 14 do Regulamento (CE) n.º 1907/2006 ([68]) **e empresas que produzem os artigos a que se refere o artigo 3.º, n.º 3, do mesmo regulamento a partir de substâncias ou misturas.**
4. Produção, transformação e distribuição de produtos alimentares		Empresas do setor alimentar na aceção do artigo 3.º, ponto 2, do Regulamento (CE) n.º 178/2002 ([69]) **que se dedicam à distribuição por grosso e à produção e transformação industriais**
5. Indústria transformadora	a) Fabrico de dispositivos médicos e dispositivos médicos para diagnóstico *in vitro*	Entidades que fabricam dispositivos médicos na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2017/745 ([70]), e entidades que fabricam dispositivos médicos para diagnóstico *in vitro* na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2017/746 ([71]), com exceção das entidades que fabricam dispositivos

68 Regulamento (CE) n.º 1907/2006 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2006, relativo ao registo, avaliação, autorização e restrição dos produtos químicos (REACH), que cria a Agência Europeia dos Produtos Químicos, que altera a Diretiva 1999/45/CE e revoga o Regulamento (CEE) n.º 793/93 do Conselho e o Regulamento (CE) n.º 1488/94 da Comissão, bem como a Diretiva 76/769/CEE do Conselho e as Diretivas 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE da Comissão (JO L 396 de 30.12.2006, p. 1).

69 Regulamento (CE) n.º 178/2002 do Parlamento Europeu e do Conselho, de 28 de janeiro de 2002, que determina os princípios e normas gerais da legislação alimentar, cria a Autoridade Europeia para a Segurança dos Alimentos e estabelece procedimentos em matéria de segurança dos géneros alimentícios (JO L 31 de 1.2.2002, p. 1).

70 Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1).

71 Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico *in vitro* e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).

		médicos referidas no anexo I, ponto 5.
	b) Fabrico de equipamentos informáticos, eletrónicos e óticos	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 26, da NACE Rev. 2
	c) Fabrico de equipamentos elétricos	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 27, da NACE Rev. 2
	d) Fabrico de máquinas e equipamentos (não especificados)	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 28, da NACE Rev. 2
	e) Fabrico de veículos automóveis, reboques e semirreboques	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 29, da NACE Rev. 2
	f) Fabrico de outros equipamentos de transporte	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 30, da NACE Rev. 2
6. Prestadores de serviços digitais		— Fornecedores de mercados em linha
		— Fornecedores de motores de pesquisa em linha
		— Fornecedores de plataformas de serviços de redes sociais