DIRETIVAS

DIRETIVA (UE) 2022/2555 DO PARLAMENTO EUROPEU E DO CONSELHO

de 14 de dezembro de 2022

relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2)

(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 Banco Central Europeu ([1]),

Tendo em conta o parecer do Comité Económico e Social Europeu ([2]),

Após consulta ao Comité das Regiões,

Deliberando de acordo com o processo legislativo ordinário ([3]),

Considerando o seguinte:

(1) A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([4]) tinha por objetivo desenvolver as capacidades de cibersegurança em toda a União, atenuar as ameaças aos sistemas de rede e informação utilizados para prestar serviços essenciais em setores-chave e garantir a continuidade de tais serviços em face de incidentes, contribuindo assim para a segurança da União e para o eficaz funcionamento da sua economia e sociedade.

(2) Desde a entrada em vigor da Diretiva (UE) 2016/1148, foram alcançados progressos significativos no sentido de aumentar a ciber-resiliência da União. A avaliação dessa diretiva revelou que esta funcionou como um catalisador para a abordagem institucional e regulamentar para a cibersegurança na União, abrindo as portas a uma mudança significativa das mentalidades. A referida diretiva assegurou a conclusão de quadros nacionais em matéria de segurança dos sistemas de rede e informação, mediante a definição de estratégias nacionais em matéria de segurança dos sistemas de rede e informação, o estabelecimento de capacidades nacionais e a aplicação de medidas regulamentares que abrangem as infraestruturas e as entidades essenciais identificadas por cada Estado-Membro. A Diretiva (UE) 2016/1148 contribuiu igualmente para a cooperação a nível da União por via da criação do grupo de cooperação e da rede de equipas nacionais de resposta a incidentes de segurança informática. Não obstante esses resultados, a avaliação da Diretiva (UE) 2016/1148 revelou deficiências intrínsecas que a impedem de responder de forma eficaz a desafios atuais e emergentes no domínio da cibersegurança.

(3) Com a rápida transformação digital e interligação da sociedade, nomeadamente nos intercâmbios transfronteiriços, os sistemas de rede e informação passaram a ocupar um lugar central na vida quotidiana. Essa evolução originou um alargamento do cenário de ciberameaças, 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 estão a aumentar e constituem uma grave ameaça ao funcionamento dos sistemas de rede e informação. Consequentemente, os incidentes 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.

([1]) JO C 233 de 16.6.2022, p. 22.
([2]) JO C 286 de 16.7.2021, p. 170.
([3]) Posição do Parlamento Europeu de 10 de novembro de 2022 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 28 de novembro de 2022.
([4]) 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 de 19.7.2016, p. 1).

Por conseguinte, a preparação e a eficácia no domínio da cibersegurança nunca foram tão importantes para o bom funcionamento do mercado interno como agora. Além disso, a cibersegurança é um fator essencial que permite a muitos setores críticos adotar com êxito a transformação digital e tirar pleno partido das vantagens económicas, sociais e sustentáveis da digitalização.

(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 significativas variam consideravelmente entre os Estados-Membros em termos do tipo de requisitos, do seu grau de pormenor e do método de supervisão. Essas disparidades implicam custos adicionais e criam dificuldades para as entidades 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, a eventual inadequação na conceção ou aplicação de requisitos de cibersegurança num Estado-Membro terá, provavelmente, repercussões no nível de cibersegurança de outros Estados-Membros, em especial em virtude da intensidade dos 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. Existem divergências semelhantes na aplicação das disposições da Diretiva (UE) 2016/1148 em matéria de supervisão e execução.

(5) Todas essas divergências implicam uma fragmentação do mercado interno e podem prejudicar o seu funcionamento, afetando, em especial, a prestação transfronteiriça de serviços e o nível de ciber-resiliência devido à aplicação de uma variedade de medidas. Em última análise, essas divergências poderiam conduzir a uma maior vulnerabilidade de alguns Estados-Membros às ciberameaças, com potenciais repercussões em toda a União. 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 medidas de execução eficazes que são fundamentais para a execução efetiva dessas obrigações. Por conseguinte, a Diretiva (UE) 2016/1148 deverá ser revogada e substituída pela presente diretiva.

(6) Com a revogação da Diretiva (UE) 2016/1148, o âmbito de aplicação por setor deverá ser alargado a uma parte mais vasta da economia a fim de assegurar uma cobertura exaustiva dos setores e serviços de importância vital para as atividades económicas e sociais fundamentais no mercado interno. Em especial, a presente diretiva tem por objetivo colmatar as lacunas da diferenciação entre operadores de serviços essenciais e prestadores de serviços digitais, que se revelou obsoleta, uma vez que não reflete a importância dos setores ou serviços para as atividades económicas e sociais no mercado interno.

(7) Nos termos da Diretiva (UE) 2016/1148, cabia aos Estados-Membros identificar as entidades que cumpriam os critérios de classificação como operadores de serviços essenciais. 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 às medidas de gestão de riscos de cibersegurança e às obrigações de notificação, há que estabelecer um critério uniforme para identificar as entidades abrangidas pelo âmbito da presente diretiva. Tal critério deverá consistir na aplicação da regra da limitação com base na dimensão da empresa, nos termos da qual todas as entidades que sejam consideradas médias empresas nos termos do artigo 2.º do anexo da Recomendação 2003/361/CE da Comissão ([5]), ou que excedam os limiares relativos às médias empresas previstos no n.º 1 desse artigo, e que atuam nos setores e que prestam os tipos de serviços ou exerçam atividades abrangidos pela presente diretiva

([5]) 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).

estão abrangidas pelo seu âmbito. Os Estados-Membros deverão igualmente prever que determinadas pequenas empresas e microempresas, na aceção do artigo 2.º, n.ºs 2 e 3, do referido anexo, que preencham critérios específicos indicativos de um papel fundamental para a sociedade, a economia ou para setores ou tipos de serviços específicos sejam abrangidas pelo âmbito da presente diretiva.

(8) A exclusão de entidades da administração pública do âmbito da presente diretiva deverá aplicar-se às entidades cujas atividades sejam predominantemente exercidas nos domínios da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo a prevenção, investigação, deteção e repressão de infrações penais. No entanto, as entidades da administração pública cujas atividades estejam apenas marginalmente relacionadas com esses domínios não deverão ser excluídas do âmbito de aplicação da presente diretiva. Para efeitos da presente diretiva, não se considera que as entidades com competências regulamentares exercem atividades no domínio da aplicação da lei, pelo que não ficam excluídas com esse fundamento do âmbito de aplicação da presente diretiva. As entidades da administração pública estabelecidas em conjunto com um país terceiro em conformidade com um acordo internacional estão excluídas do âmbito de aplicação da presente diretiva. A presente diretiva não se aplica às missões diplomáticas e consulares dos Estados-Membros em países terceiros nem aos seus sistemas de rede e informação, na medida em que esses sistemas estejam localizados nas instalações da missão ou sejam explorados para utilizadores num país terceiro.

(9) Os Estados-Membros deverão poder tomar as medidas necessárias para garantir a proteção dos interesses essenciais da segurança nacional, salvaguardar a ordem e a segurança públicas e permitir a prevenção, a investigação, a deteção e a repressão das infrações penais. Para o efeito, os Estados-Membros deverão poder isentar entidades específicas que exercem atividades nos domínios da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo atividades relacionadas com a prevenção, investigação, deteção e repressão de infrações penais, da obrigação de cumprir certas obrigações estabelecidas na presente diretiva no que diz respeito a essas atividades. Caso uma entidade preste serviços exclusivamente a uma entidade da administração pública excluída do âmbito de aplicação da presente diretiva, os Estados-Membros deverão poder isentar essa entidade de cumprir determinadas obrigações estabelecidas na presente diretiva no que diz respeito a esses serviços. Além disso, nenhum Estado-Membro deverá ser obrigado a prestar informações cuja divulgação seja contrária aos interesses essenciais do Estado– Membro em matéria de segurança nacional, segurança pública ou defesa. Nesse contexto, deverão ser tidas em conta as regras nacionais 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» (do inglês, *traffic light protocol*). O protocolo «sinalização luminosa» deve ser entendido como um meio de fornecer informações sobre possíveis limitações à disseminação posterior de informações. É utilizado em quase todas as equipas de resposta a incidentes de segurança informática (CSIRT, do inglês, *computer security incident response teams*) e em alguns centros de partilha e análise de informações.

(10) Embora a presente diretiva se aplique a entidades que exercem atividades de produção de eletricidade a partir de centrais nucleares, algumas dessas atividades podem estar ligadas à segurança nacional. Se for esse o caso, um Estado-Membro deverá poder exercer a sua responsabilidade de salvaguardar a segurança nacional no que diz respeito a essas atividades, incluindo as atividades no âmbito da cadeia de valor nuclear, em conformidade com os Tratados.

(11) Algumas entidades exercem atividades no domínio da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo a prevenção, a investigação, a deteção e a repressão das infrações penais, prestando simultaneamente serviços de confiança. Os prestadores de serviços de confiança abrangidos pelo âmbito de aplicação do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([6]) deverão ser abrangidos pelo âmbito de aplicação da presente diretiva, a fim de garantir o mesmo nível de requisitos de segurança e supervisão que o anteriormente estabelecido no referido regulamento a respeito dos prestadores de serviços de confiança. Em consonância com a exclusão de determinados serviços específicos do Regulamento (UE) n.º 910/2014, a presente diretiva não deverá aplicar-se à oferta de serviços de confiança utilizados exclusivamente dentro de sistemas fechados que decorram do direito nacional ou de acordos entre um grupo definido de participantes.

([6]) 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).

(12) Os prestadores de serviços postais, tal como definidos na Diretiva 97/67/CE do Parlamento Europeu e do Conselho ([7]), incluindo os prestadores de serviços de correio, 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, tendo simultaneamente em conta o grau da sua dependência dos sistemas de rede e informação. Os serviços de transporte que não sejam prestados em conjunto com uma dessas atividades deverão ser excluídos do âmbito dos serviços postais.

(13) Tendo em conta a intensificação e a crescente sofisticação das ciberameaças, os Estados-Membros deverão procurar assegurar que as entidades excluídas do âmbito de aplicação da presente diretiva atinjam um elevado nível de cibersegurança e apoiar a aplicação de medidas equivalentes de gestão dos riscos de cibersegurança que reflitam a natureza sensível dessas entidades.

(14) O direito da União em matéria de proteção de dados e o direito da União em matéria de privacidade são aplicáveis a qualquer tratamento de dados pessoais realizado ao abrigo da presente diretiva. Em especial, a presente diretiva não prejudica o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([8]) e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([9]). Por conseguinte, a presente diretiva não deverá afetar, nomeadamente, as funções e os poderes das autoridades competentes para controlar o cumprimento do direito da União em matéria de proteção de dados e do direito da União em matéria de privacidade aplicáveis.

(15) As entidades abrangidas pelo âmbito de aplicação da presente diretiva, para efeitos de cumprimento das obrigações relativas às medidas de gestão dos riscos de cibersegurança e à notificação, deverão ser classificadas em duas categorias, entidades essenciais e entidades importantes, refletindo a medida em que são fundamentais no que respeita ao seu setor ou ao tipo de serviço que prestam, bem como a sua dimensão. A este respeito, deverão ser tidas devidamente em conta quaisquer avaliações de risco setoriais ou orientações pertinentes emitidas pelas autoridades competentes, quando aplicável. Os regimes de supervisão e de execução aplicáveis a essas duas categorias deverão 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.

(16) A fim de evitar que as entidades que têm empresas parceiras ou que são empresas associadas sejam consideradas entidades essenciais ou importantes se tal for desproporcionado, os Estados-Membros podem ter em conta o grau de independência de que goza uma entidade em relação às suas empresas parceiras ou associadas aquando da aplicação do artigo 6.º, n.º 2, do anexo da Recomendação 2003/361/CE. Em especial, os Estados-Membros podem ter em conta o facto de uma entidade ser independente das suas empresas parceiras ou associadas em termos de sistemas de rede e informação que essa entidade utiliza na prestação dos seus serviços e em termos dos serviços que presta. Nessa base, se for caso disso, os Estados-Membros podem considerar que tal entidade não é uma média empresa nos termos do artigo 2.º do anexo da Recomendação 2003/361/CE, ou não excede os limiares relativos a uma média empresa previstos no n.º 1 desse artigo, se, após ter em conta o grau de independência dessa entidade, essa entidade não teria sido considerada uma média empresa ou não teria excedido esses limiares no caso de apenas serem tidos em conta os seus próprios dados. Tal não afeta as obrigações previstas na presente diretiva para as empresas parceiras e associadas abrangidas pelo âmbito de aplicação da presente diretiva.

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

([7]) 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 à melhoria da qualidade de serviço (JO L 15 de 21.1.1998, p. 14).

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

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

(18) A fim de assegurar uma panorâmica clara das entidades abrangidas pelo âmbito de aplicação da presente diretiva, os Estados-Membros deverão estabelecer uma lista de entidades essenciais e importantes, bem como de entidades que prestam serviços de registo de nomes de domínio. Para o efeito, os Estados-Membros deverão exigir que as entidades apresentem, pelo menos, as seguintes informações às autoridades competentes, a saber, o nome, o endereço e os dados de contacto atualizados, incluindo os endereços de correio eletrónico, as gamas de endereços IP e os números de telefone da entidade e, se aplicável, o setor e subsetor pertinentes referidos nos anexos, bem como, se aplicável, uma lista dos Estados-Membros em que prestam serviços abrangidos pelo âmbito da presente diretiva. Nesse sentido, a Comissão, com a assistência da Agência da União Europeia para a Cibersegurança (ENISA), deverá fornecer, sem demora injustificada, orientações e modelos no que diz respeito às obrigações de enviar informações. A fim de facilitar a elaboração e atualização da lista de entidades essenciais e importantes, bem como de entidades que prestam serviços de registo de nomes de domínio, os Estados-Membros deverão poder estabelecer mecanismos nacionais para que as entidades se registem. Caso os registos existam a nível nacional, os Estados-Membros podem decidir quais os mecanismos adequados que permitem a identificação das entidades abrangidas pelo âmbito de aplicação da presente diretiva.

(19) Os Estados-Membros deverão ser responsáveis por comunicar à Comissão, pelo menos, o número de entidades essenciais e importantes para cada setor e subsetor referidos nos anexos, bem como informações pertinentes sobre o número de entidades identificadas e a disposição, de entre as previstas na presente diretiva, com base na qual foram identificadas, e o tipo de serviço que prestam. Os Estados-Membros são incentivados a proceder ao intercâmbio de informações com a Comissão sobre entidades essenciais e importantes e, em caso de incidente de cibersegurança em grande escala, informações pertinentes, como o nome da entidade em causa.

(20) Em cooperação com o grupo de cooperação e após consulta das partes interessadas pertinentes, a Comissão deverá fornecer orientações sobre a aplicação dos critérios relativos às microempresas e às pequenas empresas para avaliar se elas são abrangidas pelo âmbito da presente diretiva. A Comissão deverá também garantir o fornecimento de orientações adequadas a todas as microempresas e pequenas empresas abrangidas pelo âmbito de aplicação da presente diretiva. A Comissão, com a assistência dos Estados-Membros, deverá colocar à disposição das microempresas e das pequenas empresas informações a este respeito.

(21) A Comissão poderá fornecer orientações para apoiar os Estados-Membros na aplicação das disposições da presente diretiva relativas ao âmbito de aplicação e na avaliação da proporcionalidade das medidas a adotar nos termos da presente diretiva, em particular no que toca a entidades com modelos de negócio ou ambientes operacionais complexos, em que uma entidade pode simultaneamente preencher os critérios atribuídos a entidades essenciais e a entidades importantes ou pode simultaneamente exercer algumas atividades abrangidas pelo âmbito de aplicação da presente diretiva e algumas atividades excluídas do mesmo.

(22) A presente diretiva estabelece a base de referência para as medidas de gestão dos riscos de cibersegurança e as obrigações de notificação nos 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 necessários outros atos jurídicos da União setoriais relativos às medidas de gestão dos riscos de cibersegurança e às obrigações de notificação para garantir um elevado nível de cibersegurança em toda a União, a Comissão deverá avaliar se essas disposições adicionais poderão ser definidas num ato de execução nos termos da presente diretiva. Caso esses atos de execução não sejam adequados para o efeito, os atos jurídicos setoriais da União poderão contribuir para assegurar um elevado nível de cibersegurança em toda a União, tomando simultaneamente em plena consideração as especificidades e complexidades dos setores em causa. Nesse sentido, a presente diretiva não obsta à adoção de atos jurídicos setoriais adicionais da União relacionados com medidas de gestão dos riscos de cibersegurança e obrigações de notificação que tenham em devida conta a necessidade de um quadro de cibersegurança exaustivo e coerente. A presente diretiva não prejudica as atuais competências de execução atribuídas à Comissão em vários setores, incluindo transportes e energia.

(23) Nos casos em que um ato jurídico setorial da União inclua disposições que exijam que entidades essenciais e importantes adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes significativos, e, se tais exigências forem, na prática, pelo menos equivalentes às obrigações estabelecidas na presente diretiva, essas

disposições, incluindo em matéria de supervisão e execução, deverão aplicar-se a essas entidades. Se um ato jurídico setorial da União não abranger todas as entidades de um setor específico abrangido pelo âmbito de aplicação da presente diretiva, as disposições pertinentes da presente diretiva deverão continuar a aplicar-se às entidades não abrangidas pelo referido ato.

(24) Sempre que as disposições de um ato jurídico setorial da União exijam que as entidades essenciais ou importantes cumpram obrigações de notificação que sejam pelo menos equivalentes na prática às obrigações de notificação estabelecidas na presente diretiva, deverá ser assegurada a coerência e a eficácia do tratamento das notificações de incidentes. Para o efeito, as disposições do ato jurídico setorial da União sobre a notificação de incidentes deverão proporcionar às CSIRT, às autoridades competentes ou aos pontos de contacto únicos em matéria de cibersegurança (pontos de contacto únicos) ao abrigo da presente diretiva um acesso imediato às notificações de incidentes apresentadas em conformidade com o ato jurídico setorial da União. Em especial, esse acesso imediato pode ser assegurado se as notificações de incidentes forem reencaminhadas sem demora injustificada à CSIRT, à autoridade competente ou ao ponto de contacto único nos termos da presente diretiva. Se for caso disso, os Estados-Membros deverão criar um mecanismo de comunicação automática e direta que assegure a partilha sistemática e imediata de informações com as CSIRT, as autoridades competentes ou os pontos de contacto único sobre o tratamento dessas notificações de incidentes. A fim de simplificar a comunicação de informações e de aplicar o mecanismo de comunicação automática e direta, os Estados-Membros poderão, em conformidade com o ato jurídico setorial da União, utilizar um ponto de entrada único.

(25) Os atos jurídicos setoriais da União que prevejam 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 ao abrigo desses atos exerçam as suas competências de supervisão e execução em relação a essas medidas ou obrigações com a assistência das autoridades competentes nos termos da presente diretiva. As autoridades competentes em causa poderão estabelecer acordos de cooperação para esse 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 em matéria de supervisão e execução entre as autoridades competentes, incluindo o acesso a informações relacionadas com o ciberespaço solicitadas pelas autoridades competentes nos termos da presente diretiva.

(26) Sempre que atos jurídicos setoriais da União exijam ou proporcionem incentivos às entidades para notificarem ciberameaças significativas, os Estados-Membros deverão também incentivar a partilha de ciberameaças significativas com as CSIRT, as autoridades competentes ou os pontos de contacto únicos ao abrigo da presente diretiva, a fim de assegurar um maior nível de sensibilização desses organismos para o panorama das ciberameaças e de permitir-lhes dar resposta, de forma eficaz e atempada, caso as ciberameaças significativas se materializem.

(27) Os futuros atos jurídicos setoriais da União deverão ter devidamente em conta as definições e o quadro de supervisão e execução estabelecidos na presente diretiva.

(28) O Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho ([10]) deverá ser considerado um ato jurídico setorial da União para efeitos da presente diretiva no que diz respeito às entidades financeiras. As disposições do Regulamento (UE) 2022/2554 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, às obrigações de notificação de incidentes de caráter severo relacionados com as TIC, bem como as relativas a testes de resiliência operacional digital, acordos de partilha de informações e riscos de terceiros no domínio das TIC, deverão ser aplicadas em vez das disposições previstas na presente diretiva. Por conseguinte, os Estados-Membros não deverão aplicar as disposições da presente diretiva em matéria de obrigações de gestão dos riscos de cibersegurança e de notificação, e em matéria de supervisão e execução, relativas às entidades financeiras abrangidas pelo Regulamento (UE) 2022/2554. 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 (UE) 2022/2554 permite que as autoridades europeias de supervisão (AES) e as autoridades competentes ao abrigo desse regulamento participem nas atividades do grupo de cooperação, e que troquem informações e cooperem com os pontos de contacto únicos, bem como com as CSIRT e as autoridades competentes ao abrigo da presente diretiva. As autoridades competentes ao abrigo do Regulamento (UE) 2022/2554 também deverão transmitir informações pormenorizadas sobre incidentes graves

([10]) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (ver página 1 do presente Jornal Oficial).

relacionados com as TIC e, quando pertinente, com ciberameaças significativas às autoridades competentes, às CSIRT ou os pontos de contacto únicos nos termos da presente diretiva. Tal é possível através de um acesso imediato a notificações de incidentes e do respetivo reencaminhamento quer diretamente quer através de um ponto de entrada único. Adicionalmente, os Estados-Membros deverão continuar a incluir o setor financeiro nas respetivas estratégias de cibersegurança e as CSIRT podem contemplar o setor financeiro nas suas atividades.

(29) A fim de evitar lacunas ou duplicações das obrigações em matéria de cibersegurança impostas às entidades do setor da aviação, as autoridades nacionais nos termos dos Regulamentos (CE) n.º 300/2008 ([11]) e (UE) 2018/1139 ([12]) 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 da conformidade dessas medidas a nível nacional. O cumprimento por uma entidade dos requisitos de segurança estabelecidos nos Regulamentos (CE) n.º 300/2008 e (UE) 2018/1139 e nos atos delegados e de execução pertinentes adotados nos termos desses regulamentos poderá ser tida em conta pelas autoridades competentes ao abrigo da presente diretiva como constituindo o cumprimento dos requisitos correspondentes estabelecidos na presente diretiva.

(30) Tendo em conta as interligações entre a cibersegurança e a segurança física das entidades, importa assegurar uma abordagem coerente entre a Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho ([13]) e a presente diretiva. Para tal, as entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557 deverão ser consideradas entidades essenciais no âmbito da presente diretiva. Além disso, cada Estado-Membro deverá garantir que a sua estratégia nacional em matéria de cibersegurança preveja um quadro político para o reforço da cooperação nos Estados-Membros entre as suas autoridades competentes nos termos da presente diretiva e as autoridades competentes nos termos da Diretiva (UE) 2022/2557 no contexto da partilha de informações sobre os riscos, as ciberameaças e os incidentes, bem como sobre os riscos, as ameaças e os incidentes não cibernéticos e o exercício de funções de supervisão. As autoridades competentes referidas na presente diretiva e as referidas na Diretiva (UE) 2022/2557 deverão cooperar e trocar informações, sem demora injustificada, especialmente no que respeita à identificação de entidades críticas, riscos, ciberameaças e incidentes, bem como no que respeita a riscos, ameaças e incidentes não cibernéticos que afetem entidades críticas, inclusive sobre medidas físicas e de cibersegurança adotadas por entidades críticas, bem como 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 nos termos da presente diretiva e da Diretiva (UE) 2022/2557 e a fim de minimizar os encargos administrativos para as entidades em causa, essas autoridades competentes deverão procurar harmonizar os modelos de notificação de incidentes e os processos de supervisão. Se for caso disso, as autoridades competentes nos termos da Diretiva (UE) 2022/2557 deverão poder solicitar às autoridades competentes ao abrigo da presente diretiva que exerçam as suas competências de supervisão e execução em relação a uma entidade que também seja identificada como entidade crítica nos termos da Diretiva (UE) 2022/2557. As autoridades competentes nos termos da presente diretiva e as autoridades competentes nos termos da Diretiva (UE) 2022/2557 deverão, se possível em tempo real, cooperar e trocar informações para este fim.

(31) As entidades pertencentes ao setor das infraestruturas digitais baseiam-se por natureza nos sistemas de rede e informação, pelo que as obrigações impostas a essas entidades nos termos da presente diretiva deverão atender de forma abrangente à segurança física desses sistemas, no quadro das suas medidas de gestão dos riscos de cibersegurança e das obrigações de notificação. Uma vez que essas matérias são abrangidas pela presente diretiva, as obrigações estabelecidas nos capítulos III, IV e VI da Diretiva (UE) 2022/2557 não se aplicam a tais entidades.

([11]) 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).

([12]) 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).

([13]) Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas, e que revoga a Diretiva 2008/114/CE do Conselho (ver página 164 do presente Jornal Oficial).

(32) A proteção e a conservação de um sistema de nomes de domínio (DNS, do inglês, *domain name system*) fiável, resiliente e seguro são fatores cruciais para manter a integridade da Internet, sendo igualmente essenciais 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 registos de nomes de domínio de topo (TLD, do inglês *top-level-domain*) e a prestadores de serviços de DNS que devem ser entendidos como entidades que prestam serviços de resolução recursiva de nomes de domínio disponíveis ao público para utilizadores finais de Internet ou serviços de resolução com autoridade para nomes de domínio para utilização de terceiros. A presente diretiva não deverá ser aplicável a servidores de nomes raiz.

(33) Os serviços de computação em nuvem deverão abranger serviços digitais que permitam a administração a pedido e um amplo acesso remoto a um conjunto modulável e adaptável de recursos de computação partilháveis, inclusive quando esses recursos são distribuídos por várias localizações. Os 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, do inglês *Infrastructure as a Service*), a plataforma como serviço (PaaS, do inglês *Platform as a Service*), o software como serviço (SaaS, do inglês *Software as a Service*) e a rede como serviço (NaaS, do inglês *Network as a Service*). Os modelos de implantação da computação em nuvem deverão incluir soluções de nuvem privada, comunitária, pública e híbrida. Os serviços e os modelos de implantação de computação em nuvem 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 client*), nomeadamente telemóveis, tabletes, computadores portáteis e 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 fornecidos 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.

(34) Dada a emergência de tecnologias inovadoras e de novos modelos de negócio, espera-se que surjam novos serviços e modelos de implantação da computação em nuvem no mercado interno 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»).

(35) Os serviços oferecidos por prestadores de serviços de centro de dados nem sempre serão prestados sob a forma de um 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 dos sistemas de rede e informação, a presente diretiva, por conseguinte, deverá abranger 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» deverá abranger a prestação de um serviço que englobe estruturas ou grupos de estruturas dedicados ao alojamento, à interligação e à operação centralizadas de equipamento de redes e tecnologias da informação (TI) 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 deverá aplicar aos centros de dados internos das empresas, detidos e geridos pela entidade em causa, para os seus próprios fins.

(36) As atividades de investigação desempenham um papel fundamental no desenvolvimento de novos produtos e processos. Muitas dessas atividades são realizadas por entidades que partilham, divulgam ou exploram os resultados da sua investigação para fins comerciais. Por conseguinte, essas entidades podem ser intervenientes importantes nas cadeias de valor, pelo que a segurança dos seus sistemas de rede e informação faz parte integrante da cibersegurança global do mercado interno. Os organismos de investigação deverão ser entendidos como entidades que concentram a parte essencial das suas atividades na realização de investigação aplicada ou no desenvolvimento experimental, na

aceção do Manual de Frascati 2015 da Organização de Cooperação e de Desenvolvimento Económicos: Orientações para a recolha e comunicação de dados sobre a investigação e o desenvolvimento experimental, com vista a explorar os seus resultados para fins comerciais, como o fabrico ou o desenvolvimento de um produto ou processo, ou a prestação de um serviço, ou a respetiva comercialização.

(37) As 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 em setores como o 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 do seu programa espacial. 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 intensificação dos ciberataques durante a pandemia de COVID-19 revelou a vulnerabilidade das nossas sociedades, cada vez mais interdependentes perante riscos com baixa probabilidade de ocorrência.

(38) 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 deverão poder designar ou estabelecer uma ou mais autoridades competentes responsáveis pela cibersegurança e pelas funções de supervisão nos termos da presente diretiva.

(39) 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 responsável pela coordenação das questões relativas à segurança dos sistemas de rede e informação e pela cooperação transfronteiriça a nível da União.

(40) Os pontos de contacto únicos deverão assegurar uma cooperação transfronteiriça eficaz com as autoridades competentes de outros Estados-Membros e, se for caso disso, com a Comissão e a ENISA. Os pontos de contacto únicos, por conseguinte, deverão ser incumbidos do reencaminhamento das notificações de incidentes significativos com impacto transfronteiriço para os pontos de contacto únicos de outros Estados-Membros afetados, a pedido da CSIRT ou da autoridade competente. A nível nacional, os pontos de contacto únicos deverão permitir uma cooperação transetorial harmoniosa com outras autoridades competentes. Os pontos de contacto únicos poderão ser também os destinatários de informações sobre incidentes respeitantes a entidades do setor financeiro fornecidas pelas autoridades competentes nos termos do Regulamento (UE) 2022/2554, informações essas que deverão poder transmitir, conforme adequado, às CSIRT ou às autoridades competentes nos termos da presente diretiva.

(41) Os Estados-Membros deverão estar adequadamente equipados, em termos de capacidade técnica e organizativa, para evitar, detetar, enfrentar e atenuar os incidentes e os riscos. Por conseguinte, deverão criar ou designar uma ou mais CSIRT ao abrigo da presente diretiva e assegurar que estas dispõem dos recursos e capacidades técnicas adequados. As CSIRT deverão preencher os requisitos estabelecidos na presente diretiva para garantir capacidades efetivas e compatíveis para fazer face aos incidentes e aos riscos e para assegurar uma cooperação eficaz a nível da União. Os Estados-Membros deverão poder designar como CSIRT equipas de resposta a emergências informáticas (CERT, do inglês *computer emergency response teams*) existentes. No intuito de melhorar a relação de confiança entre as entidades e as CSIRT, se uma autoridade competente dispuser de uma CSIRT, os Estados-Membros deverão poder ponderar a separação funcional entre as funções operacionais desempenhadas pelas CSIRT, especialmente no que respeita à partilha de informações e à assistência prestada às entidades, e as atividades de supervisão das autoridades competentes.

(42) As CSIRT são responsáveis pelo tratamento de incidentes. Tal inclui o tratamento de grandes volumes de dados por vezes sensíveis. Os Estados-Membros deverão assegurar que as CSIRT disponham de uma infraestrutura para a partilha e o tratamento de informações, bem como de pessoal bem equipado, que garanta a confidencialidade e a fiabilidade das suas operações. As CSIRT podem igualmente adotar códigos de conduta a este respeito.

(43) No que respeita a dados pessoais, as CSIRT deverão poder facultar, em conformidade com o Regulamento (UE) 2016/679, a pedido de uma entidade essencial ou importante, uma análise proativa dos sistemas de rede e informação utilizados para prestarem os serviços da entidade. Se aplicável, os Estados-Membros deverão procurar garantir que todas as CSIRT setoriais possuam o mesmo nível de capacidades técnicas. Os Estados-Membros devem poder solicitar a assistência da ENISA na criação das suas CSIRT.

(44) As CSIRT deverão ter capacidade para, a pedido de uma entidade essencial ou importante, monitorizar todos os ativos da entidade com acesso à Internet, tanto nas instalações como fora delas, a fim de identificar, compreender e gerir os riscos globais organizacionais da entidade face a recém-identificadas exposições ou a vulnerabilidades críticas da cadeia de abastecimento. A entidade deverá ser incentivada a comunicar à CSIRT se opera uma interface de gestão privilegiada, uma vez que tal pode afetar a rapidez da adoção de medidas de atenuação.

(45) 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, para efeitos do exercício das suas funções, as CSIRT e as autoridades competentes deverão poder trocar informações, incluindo dados pessoais, com equipas nacionais de resposta a incidentes de segurança informática ou com autoridades competentes de países terceiros, desde que estejam preenchidas as condições previstas no direito da União em matéria de proteção de dados para as transferências de dados pessoais para países terceiros, nomeadamente as previstas no artigo 49.º do Regulamento (UE) 2016/679.

(46) É essencial assegurar recursos adequados para cumprir os objetivos da presente diretiva e para permitir às autoridades competentes e às CSIRT desempenhar as funções aqui estabelecidas. Os Estados-Membros podem introduzir a nível nacional um mecanismo de financiamento para cobrir as despesas necessárias relacionadas com o exercício das funções das entidades públicas responsáveis pela cibersegurança no Estado-Membro nos termos da presente diretiva. Esse mecanismo deverá respeitar o direito da União, deverá ser proporcionado e não discriminatório e deverá ter em conta diferentes abordagens para a prestação de serviços seguros.

(47) 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.

(48) A fim de alcançar e manter um elevado nível de cibersegurança, as estratégias nacionais de cibersegurança exigidas pela presente diretiva deverão consistir em quadros coerentes que estabeleçam objetivos e prioridades estratégicos no domínio da cibersegurança e a governação para os alcançar. Essas estratégias podem ser compostas por um ou mais instrumentos legislativos ou não legislativos.

(49) As políticas de ciber-higiene garantem as bases para a proteção da segurança das infraestruturas dos sistemas de rede e informação, do hardware, do software e das aplicações em linha, bem como dos dados das empresas ou dos utilizadores finais dos quais as entidades dependem. As políticas de ciber-higiene que comportam um conjunto comum de práticas de base, incluindo atualizações de software e hardware, alterações de palavra-passe, gestão de novas instalações, limitação das contas de acesso a nível de administrador e salvaguarda de dados, asseguram um quadro pró-ativo de preparação e de proteção e segurança gerais em caso de incidentes ou ciberameaças. A ENISA deverá acompanhar e analisar as políticas de ciber-higiene dos Estados-Membros.

(50) A sensibilização para a cibersegurança e a ciber-higiene são essenciais para melhorar o nível de cibersegurança na União, em especial tendo em conta o número crescente de dispositivos conectados que são cada vez mais utilizados em ciberataques. Deverão ser envidados esforços para aumentar a sensibilização global para os riscos relacionados com esses dispositivos, enquanto as avaliações a nível da União poderão contribuir para assegurar um entendimento comum desses riscos no mercado interno.

(51) Os Estados-Membros deverão incentivar a utilização de qualquer tecnologia inovadora, incluindo a inteligência artificial, cuja utilização possa melhorar a deteção e a prevenção de ciberataques, permitindo que os recursos sejam desviados para os ciberataques de forma mais eficaz. Por conseguinte, os Estados-Membros deverão incentivar, no âmbito da sua estratégia nacional de cibersegurança, as atividades de investigação e desenvolvimento destinadas a promover a utilização dessas tecnologias, em especial as relacionadas com ferramentas automatizadas ou semiautomatizadas no domínio da cibersegurança, e, quando pertinente, a partilha dos dados necessários para a formação dos utilizadores dessas tecnologias e para a sua melhoria. A utilização de qualquer tecnologia inovadora, incluindo a inteligência artificial, deverá respeitar o direito da União em matéria de proteção de dados, incluindo os princípios da proteção de dados em matéria de exatidão dos dados, minimização dos dados, equidade e transparência, bem como a segurança dos dados, como a encriptação de ponta. Os requisitos de proteção de dados desde a conceção e por defeito estabelecidos no Regulamento (UE) 2016/679 deverão ser plenamente utilizados.

(52) As ferramentas e aplicações de cibersegurança de código aberto podem contribuir para um maior grau de abertura e ter um impacto positivo na eficiência da inovação industrial. As normas abertas facilitam a interoperabilidade entre as ferramentas de segurança, beneficiando a segurança da indústria. As ferramentas e aplicações de código aberto em matéria de cibersegurança podem impulsionar a comunidade mais ampla de programadores, permitindo a diversificação de fornecedores. A fonte aberta pode conduzir a um processo de verificação mais transparente das ferramentas relacionadas com a cibersegurança e a um processo de deteção de vulnerabilidades impulsionado pela comunidade. Os Estados-Membros deverão, por conseguinte, poder promover a utilização de software de código aberto e de normas abertas, prosseguindo políticas relativas à utilização de dados abertos e de fontes abertas como parte da segurança através da transparência. As políticas que promovem a introdução e a utilização sustentável de ferramentas de cibersegurança de código aberto revestem-se de especial importância para as pequenas e médias empresas que fazem face a custos significativos de execução, os quais podem ser minimizados com a redução da necessidade de aplicações ou ferramentas específicas.

(53) Os serviços públicos estão cada vez mais ligados às redes digitais nas cidades, com o objetivo de melhorar as redes de transporte urbano, melhorar o abastecimento de água e as instalações de eliminação de resíduos e aumentar a eficiência da iluminação e do aquecimento dos edifícios. Esses serviços públicos digitais são vulneráveis a ciberataques e correm o risco, em caso de ciberataque bem-sucedido, de prejudicar em grande escala os cidadãos devido à sua interligação. Os Estados-Membros deverão elaborar uma política que aborde o desenvolvimento dessas cidades conectadas ou inteligentes e os seus potenciais impactos na sociedade, como parte da sua estratégia nacional de cibersegurança.

(54) Em anos recentes, a União tem enfrentado um aumento exponencial dos ataques de *ransomware*, em que o *malware* encripta dados e sistemas e exige um pagamento de resgate para a sua libertação. A frequência e a gravidade crescentes dos ataques de *ransomware* podem ser motivadas por vários fatores, tais como os diferentes padrões de ataque, os modelos empresariais criminosos em torno do «*ransomware* como um serviço» e as criptomoedas, as exigências de resgate e o aumento dos ataques na cadeia de abastecimento. Os Estados-Membros deverão elaborar uma política que dê resposta ao aumento dos ataques de *ransomware* no âmbito da sua estratégia nacional de cibersegurança.

(55) As parcerias público-privadas (PPP) no domínio da cibersegurança podem proporcionar um quadro adequado para o intercâmbio de conhecimentos, a partilha de boas práticas e o estabelecimento de um nível comum de entendimento entre todas as partes interessadas. Os Estados-Membros deverão promover políticas que sustentem o estabelecimento de PPP específicas para a cibersegurança. Essas políticas devem clarificar, nomeadamente, o âmbito e as partes interessadas envolvidas, o modelo de governação, as opções de financiamento disponíveis e a interação entre as partes interessadas participantes no que respeita às PPP. As PPP podem mobilizar os conhecimentos especializados de entidades do setor privado para apoiar as autoridades competentes no desenvolvimento de serviços e processos de vanguarda, incluindo o intercâmbio de informações, alertas precoces, exercícios em matéria de ciberameaças e de incidentes, gestão de crises e planeamento da resiliência.

(56) Os Estados-Membros deverão abordar, nas suas estratégias nacionais de cibersegurança, as necessidades específicas das pequenas e médias empresas em matéria de cibersegurança. As pequenas e médias empresas representam, em toda a União, uma grande percentagem do mercado industrial e comercial e debatem-se frequentemente com dificuldades na adaptação às novas práticas empresariais num mundo mais ligado, e ao ambiente digital, com os empregados a trabalhar a partir de casa e negócios que se fazem cada vez mais em linha. Algumas pequenas e médias empresas enfrentam desafios de cibersegurança específicos, como uma limitada sensibilização para o ciberespaço, a falta de segurança informática à distância, o elevado custo das soluções de cibersegurança e um nível acrescido de ameaça, como o *ransomware*, em relação aos quais deverão receber orientações e assistência. As pequenas e médias empresas estão a tornar-se cada vez mais alvo de ataques nas cadeias de abastecimento devido às suas medidas menos rigorosas de gestão dos riscos de cibersegurança e de gestão de ataques, bem como ao facto de terem recursos de segurança limitados. Tais ataques na cadeia de abastecimento não só têm impacto nas pequenas e médias empresas e nas suas operações isoladamente, como também podem ter um efeito em cascata em ataques de

maior dimensão contra entidades das quais são fornecedoras. Os Estados-Membros deverão, através das suas estratégias nacionais de cibersegurança, ajudar as pequenas e médias empresas a fazer face os desafios enfrentados nas suas cadeias de abastecimento. Os Estados-Membros deverão dispor de um ponto de contacto para as pequenas e médias empresas a nível nacional ou regional, que preste orientação e assistência às pequenas e médias empresas ou as encaminhe para os organismos adequados de orientação e assistência no que diz respeito a questões relacionadas com a cibersegurança. Os Estados-Membros são também incentivados a oferecer serviços, como a configuração de sítios Web e o registo de dados, às microempresas e às pequenas empresas que não dispõem dessas capacidades.

(57) No âmbito das suas estratégias nacionais de cibersegurança, os Estados-Membros deverão adotar políticas de promoção da ciberproteção ativa como parte de uma estratégia defensiva mais ampla. Em vez de uma resposta reativa, a ciberproteção ativa consiste na prevenção, deteção, monitorização, análise e atenuação de violações da segurança da rede, de uma forma ativa, combinadas com a utilização de capacidades utilizadas dentro ou fora da rede da vítima. Tal poderá incluir a oferta por parte dos Estados-Membros de serviços ou ferramentas gratuitos a certas entidades, incluindo verificações self-service, ferramentas de deteção e serviços de retirada. A capacidade de rápida e automaticamente partilhar e compreender informações e análises de ameaças, alertas de ciberatividade e ações de resposta é fundamental para permitir unir esforços na prevenção, na deteção, na abordagem e no bloqueio bem-sucedidos de ataques contra os sistemas de rede e informação. A ciberproteção ativa baseia-se numa estratégia defensiva que exclui medidas ofensivas.

(58) Uma vez que a exploração das vulnerabilidades dos sistemas de rede e informação pode causar perturbações e danos consideráveis, a celeridade na identificação e correção de tais vulnerabilidades é um fator importante na redução dos riscos. As entidades que desenvolvem ou administram sistemas de rede e informação deverão, por conseguinte, estabelecer procedimentos adequados para fazer face a vulnerabilidades quando estas sejam detetadas. Uma vez que as vulnerabilidades são frequentemente detetadas e divulgadas por terceiros, o fabricante ou fornecedor de produtos TIC ou o prestador de serviços de TIC deverá adotar igualmente os procedimentos necessários para receber informações sobre vulnerabilidades fornecidas por terceiros. Nessa matéria, as normas internacionais ISO/IEC 30111 e ISO/IEC 29147 fornecem orientações sobre o tratamento de vulnerabilidades e a divulgação de vulnerabilidades. O reforço da coordenação entre pessoas singulares e coletivas notificadoras e os fabricantes ou fornecedores de produtos de TIC ou prestadores de serviços de TIC assume especial importância para facilitar o quadro voluntário de divulgação de vulnerabilidades. A divulgação coordenada de vulnerabilidades especifica um processo estruturado mediante o qual as vulnerabilidades são notificadas aos fabricantes ou fornecedores de produtos de TIC ou aos prestadores de serviços de TIC potencialmente vulneráveis de uma forma que lhes permite diagnosticar e corrigir as vulnerabilidades antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público. A divulgação coordenada de vulnerabilidades deverá incluir também a coordenação entre pessoas singulares ou coletivas notificadoras e o fabricante ou fornecedor de produtos de TIC ou prestador de serviços de TIC potencialmente vulneráveis no que respeita ao momento da correção e da publicação das vulnerabilidades.

(59) A Comissão, a ENISA e os Estados-Membros deverão continuar a fomentar o alinhamento com as normas internacionais e as boas práticas do setor existentes no âmbito da gestão dos riscos de cibersegurança, por exemplo, nos domínios das avaliações de segurança da cadeia de abastecimento, da partilha de informações e da divulgação de vulnerabilidades.

(60) Os Estados-Membros, em cooperação com a ENISA, 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 sujeição à responsabilidade penal, em conformidade com o direito nacional. Dado que as pessoas singulares e coletivas que investigam as vulnerabilidades podem, em alguns Estados-Membros, incorrer em responsabilidade penal e civil, os Estados-Membros são incentivados a adotar orientações sobre a não instauração de ações penais contra quem faz investigação no domínio da segurança da informação e uma isenção de responsabilidade civil para as suas atividades.

(61) Os Estados-Membros deverão designar uma das suas CSIRT como coordenadora, agindo como intermediária de confiança entre as pessoas singulares ou coletivas notificadoras e os fabricantes ou fornecedores de produtos de TIC ou os prestadores de serviços de TIC, suscetíveis de serem afetados pela vulnerabilidade, se necessário. As funções da CSIRT designada coordenadora deverão incluir a identificação e o contacto das entidades em causa, a prestação de apoio às pessoas singulares ou coletivas que notifiquem as vulnerabilidades, a negociação do calendário de divulgação e a gestão das vulnerabilidades que afetem várias entidades (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 coordenadoras deverão cooperar no âmbito da rede de CSIRT, se for caso disso.

(62) O acesso em tempo útil a informações fidedignas sobre vulnerabilidades que afetem produtos de TIC e serviços de TIC contribui para melhorar a gestão dos riscos de cibersegurança. As fontes de informações públicas sobre vulnerabilidades constituem um instrumento importante não só para as entidades e os utilizadores dos seus serviços, mas também para as autoridades competentes e as CSIRT. Por esse motivo, a ENISA deverá criar uma base de dados europeia de vulnerabilidades na qual as entidades, caibam ou não no âmbito da presente diretiva, e os seus fornecedores de sistemas de rede e informação, bem como as autoridades competentes e as CSIRT, possam, a título voluntário, divulgar e registar vulnerabilidades publicamente conhecidas, a fim de permitir que os utilizadores tomem medidas de atenuação adequadas. O objetivo desta base de dados consiste em dar resposta aos desafios únicos que os riscos colocam às entidades da União. Além disso, a ENISA deverá estabelecer um procedimento adequado relativamente ao processo de publicação, a fim de dar tempo às entidades para tomarem medidas de atenuação no que diz respeito às suas vulnerabilidades, e utilizar medidas de vanguarda em matéria de gestão dos riscos de cibersegurança, bem como conjuntos de dados de leitura ótica e as interfaces correspondentes. Para incentivar uma cultura de divulgação de vulnerabilidades, a divulgação não deverá ser efetuada em detrimento da pessoa singular ou coletiva notificadora.

(63) Embora já existam bases de dados ou registos de vulnerabilidades semelhantes, as entidades responsáveis pelo seu alojamento virtual e manutenção não estão estabelecidas na União. Uma base de dados europeia de vulnerabilidades mantida pela ENISA melhoraria a transparência do processo de publicação antes de a vulnerabilidade ser publicamente divulgada, bem como a resiliência em casos de perturbação ou interrupção da prestação de serviços semelhantes. A fim de evitar, tanto quanto possível, uma duplicação de esforços e de assegurar a complementaridade, a ENISA deverá explorar a possibilidade de celebrar acordos de cooperação estruturados com registos ou bases de dados semelhantes abrangidos pela jurisdição de um país terceiro. Em particular, a ENISA deverá explorar a possibilidade de estabelecer uma estreita cooperação com os operadores do sistema de Vulnerabilidades e Exposições Comuns (CVE, do inglês *Common Vulnerabilities and Exposures*).

(64) O grupo de cooperação deverá apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros, bem como reforçar a confiança entre eles. O grupo de cooperação deverá elaborar, de dois em dois anos, um programa de trabalho. O programa de trabalho deverá definir as ações a empreender pelo grupo de cooperação no sentido de cumprir os seus objetivos e as suas funções. O calendário para a elaboração do primeiro programa de trabalho ao abrigo da presente diretiva deverá estar alinhado com o calendário do último programa de trabalho definido nos termos da Diretiva (UE) 2016/1148, a fim de evitar potenciais perturbações das atividades do grupo de cooperação.

(65) 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, em particular no que respeita a facilitar a transposição harmonizada da presente diretiva pelos Estados-Membros, a adotar por via de uma melhor aplicação das regras existentes. O grupo de cooperação também pode fazer um levantamento das soluções nacionais para promover a compatibilidade das soluções em matéria de cibersegurança aplicadas a cada setor específico na União. Este aspeto é particularmente pertinente para os setores que têm uma natureza internacional ou transfronteiriça.

(66) O grupo de cooperação deverá 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. Poderá organizar regularmente reuniões conjuntas com partes interessadas privadas de toda a União para discutir as atividades desenvolvidas pelo grupo de cooperação e partilhar dados e pontos de vista sobre novos desafios políticos. Além disso, o grupo de cooperação deverá realizar regularmente uma avaliação do ponto da situação das ciberameaças ou incidentes, como o *ransomware*. A fim de reforçar a cooperação a nível da União, o grupo de cooperação deverá equacionar a possibilidade de convidar instituições, órgãos e organismos competentes

da União envolvidos na política de cibersegurança, como o Parlamento Europeu, a Europol, o Comité Europeu de Proteção de Dados, a Agência da União Europeia para a Segurança da Aviação, estabelecida pelo Regulamento (UE) 2018/1139, e a Agência da União Europeia para o Programa Espacial, estabelecida pelo Regulamento (UE) 2021/696 do Parlamento Europeu e do Conselho ([14]), a participarem nos seus trabalhos.

(67) As autoridades competentes e as CSIRT deverão estar habilitadas a participar em programas de intercâmbio de funcionários com outros Estados-Membros, no âmbito de um quadro específico e, se aplicável, subjacente à necessária credenciação de segurança dos funcionários que participam nesses programas de intercâmbio, no intuito de reforçar a cooperação e fortalecer a confiança entre os Estados-Membros. 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 ou da CSIRT de acolhimento.

(68) Os Estados-Membros deverão contribuir para a criação do quadro de resposta da UE a crises de cibersegurança previsto na Recomendação (UE) 2017/1584 da Comissão ([15]) por intermédio das redes de cooperação existentes, em particular a Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe), a rede de CSIRT e o grupo de cooperação. A UE-CyCLONe e a rede de CSIRT deverão cooperar com base em disposições processuais que especifiquem os pormenores dessa cooperação e evitar qualquer duplicação de tarefas. O regulamento interno da UE-CyCLONe deverá especificar as disposições de funcionamento da rede, incluindo as funções, os meios de cooperação, as interações com outros intervenientes relevantes e os modelos de partilha de informações, bem como os meios de comunicação. No atinente à gestão de crises a nível da União, as partes responsáveis deverão recorrer ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise previsto na Decisão de Execução (UE) 2018/1993 do Conselho ([16]) (mecanismo IPCR). A Comissão deverá utilizar, para esse 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, deverá ser ativado o mecanismo de resposta a situações de crise do Serviço Europeu para a Ação Externa.

(69) Nos termos do anexo da Recomendação (UE) 2017/1584, entende-se por incidente de cibersegurança em grande escala um incidente que cause um nível de perturbação superior à capacidade de resposta de um Estado-Membro ou que tenha um impacto significativo em, pelo menos, dois Estados-Membros. Consoante a sua causa e o seu impacto, os incidentes de cibersegurança em grande escala poderão agravar-se e transformar-se em verdadeiras crises que impeçam o correto funcionamento do mercado interno ou coloquem graves riscos em termos de segurança pública para entidades ou cidadãos em vários Estados-Membros ou na totalidade da União. Tendo em conta o vasto alcance e, em muitos casos, o caráter transfronteiras de tais incidentes, é importante que os Estados-Membros e as instituições, órgãos e organismos competentes da União cooperem a nível técnico, operacional e político para coordenarem eficazmente a resposta em toda a União.

(70) As crises e incidentes de cibersegurança em grande escala a nível da União exigem uma ação coordenada para assegurar uma resposta rápida e eficaz, devido ao elevado grau de interdependência entre setores e Estados-Membros. A existência de sistemas de rede e informação ciber-resilientes e a disponibilidade, confidencialidade e integridade dos dados são vitais para a segurança da União e para a proteção dos seus cidadãos, empresas e instituições contra incidentes e ciberameaças, bem como para o reforço da confiança das pessoas e das organizações na capacidade da União para promover e proteger um ciberespaço mundial, aberto, livre, estável e seguro, assente nos direitos humanos, nas liberdades fundamentais, na democracia e no Estado de direito.

([14]) Regulamento (UE) 2021/696 do Parlamento Europeu e do Conselho, de 28 de abril de 2021, que cria o Programa Espacial da União e a Agência da União Europeia para o Programa Espacial e que revoga os Regulamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 e (UE) n.º 377/2014 e a Decisão n.º 541/2014/UE (JO L 170 de 12.5.2021, p. 69).

([15]) 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).

([16]) Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (JO L 320 de 17.12.2018, p. 28).

(71) A UE-CyCLONe deverá funcionar como intermediária entre os níveis técnico e político durante crises e incidentes de cibersegurança em grande escala e deverá reforçar a cooperação a nível operacional e apoiar a tomada de decisões a nível político. Em cooperação com a Comissão, tendo em conta as suas competências no domínio da gestão de crises, a UE-CyCLONe deverá basear-se nas conclusões da rede de CSIRT e utilizar as suas próprias capacidades para criar uma análise de impacto de crises e de incidentes de cibersegurança em grande escala.

(72) Os ciberataques são de natureza transfronteiriça e um incidente significativo pode perturbar e danificar infraestruturas críticas de informação das quais depende o bom funcionamento do mercado interno. A Recomendação (UE) 2017/1584 aborda o papel de todos os intervenientes relevantes. Ademais, a Comissão é responsável, no âmbito do Mecanismo de Proteção Civil da União, criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho ([17]), por ações gerais de preparação, incluindo a gestão do Centro de Coordenação de Resposta de Emergência e do Sistema Comum de Comunicação e de Informação de Emergência, pela manutenção e pelo desenvolvimento da capacidade de análise e de conhecimento situacional, bem como pela criação e gestão da capacidade de mobilizar e enviar equipas de peritos em caso de pedido de assistência de um Estado-Membro ou de um país terceiro. A Comissão é igualmente responsável pela apresentação de relatórios analíticos sobre o mecanismo IPCR ao abrigo da Decisão de Execução (UE) 2018/1993, nomeadamente no que diz respeito ao conhecimento situacional e à preparação em matéria de cibersegurança, bem como ao conhecimento situacional e à resposta a situações de crise em matéria de agricultura, condições meteorológicas adversas, cartografia e previsões de conflitos, sistemas de alerta rápido em caso de catástrofes naturais, emergências sanitárias, vigilância de doenças infeciosas, fitossanidade, incidentes químicos, segurança dos alimentos para consumo humano e animal, saúde animal, migração, alfândega, emergências nucleares e radiológicas, e energia.

(73) Quando for caso disso, a União pode celebrar, em conformidade com o artigo 218.º do TFUE, acordos internacionais com países terceiros ou organizações internacionais que permitam e governem a sua participação em atividades específicas do grupo de cooperação, da rede de CSIRT e da UE-CyCLONe. Tais acordos deverão assegurar os interesses da União e uma proteção adequada dos dados. Tal não deverá excluir o direito dos Estados-Membros de cooperarem com países terceiros na gestão de vulnerabilidades e dos riscos de cibersegurança, facilitando a notificação e a partilha geral de informações em conformidade com o direito da União.

(74) A fim de facilitar a aplicação efetiva da presente diretiva, em particular no que se refere à gestão de vulnerabilidades, a medidas de gestão dos riscos de cibersegurança, as obrigações de notificação de informações e os mecanismos de partilha de informações relativas à cibersegurança, 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 ciberameaças, bem como de incidentes, vulnerabilidades, ferramentas e métodos, táticas, técnicas e procedimentos, grau de preparação e exercícios de gestão de crises de cibersegurança, formação, reforço de confiança e mecanismos estruturados de partilha de informações.

(75) Convém instituir avaliações pelos pares, de molde a contribuir para que sejam retirados ensinamentos das experiências partilhadas, reforçar a confiança mútua e alcançar um elevado nível comum de cibersegurança. As avaliações pelos pares podem dar azo a observações e recomendações preciosas que reforcem as capacidades globais de cibersegurança, criando uma via operacional alternativa para a partilha de boas práticas entre os Estados-Membros e contribuindo para um maior grau de maturidade dos Estados-Membros em matéria de cibersegurança. Além disso, convém que as avaliações pelos pares tenham em conta os resultados de mecanismos semelhantes, como o sistema de avaliações pelos pares da rede de CSIRT, que acrescentem valor e que evitem duplicações. A execução de avaliações pelos pares não deverá prejudicar o direito nacional ou da União em matéria de proteção de informações confidenciais ou classificadas.

(76) O grupo de cooperação deverá estabelecer uma metodologia de autoavaliação para os Estados-Membros, que vise abarcar fatores como o nível de aplicação das medidas de gestão dos riscos de cibersegurança e das obrigações de notificação, o nível de capacidades e a eficácia das autoridades competentes no desempenho das suas funções, as capacidades operacionais das CSIRT, o nível de aplicação da assistência mútua, o nível de aplicação dos acordos de partilha de informações sobre cibersegurança ou questões específicas de natureza transfronteiras ou intersectorial. Os Estados-Membros deverão ser incentivados a realizar regularmente autoavaliações e a apresentar e debater os resultados da respetiva autoavaliação no âmbito do grupo de cooperação.

([17]) Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).

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

(78) As medidas de gestão dos riscos de cibersegurança deverão ter em consideração o grau de dependência da entidade essencial ou importante em relação aos sistemas de rede e informação e incluir medidas para identificar os riscos de incidentes, para evitar e detetar os incidentes, bem como para lhes dar resposta, permitir a recuperação após estes incidentes e atenuar o seu impacto. A segurança dos sistemas de rede e informação deverá abranger a segurança dos dados armazenados, transmitidos e tratados. As medidas de gestão dos riscos de cibersegurança deverão prever uma análise sistémica que tenha em conta o fator humano, a fim de obter uma perspetiva completa da segurança do sistema de rede e informação.

(79) Uma vez que as ameaças à segurança dos sistemas de rede e informação podem ter origens diferentes, as medidas de gestão dos riscos de cibersegurança deverão basear-se numa abordagem que contempla todos os riscos e que visa a proteção dos sistemas de rede e informação e do ambiente físico contra eventos, como roubos, incêndios, inundações, falhas de telecomunicações ou de energia, ou contra o acesso físico não autorizado, bem como danos causados e interferências praticadas nas instalações de tratamento de informações da entidade essencial ou importante, que possa comprometer a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos pelos sistemas de rede e informação ou a que estes deem acesso. As medidas de gestão dos riscos de cibersegurança deverão, por conseguinte, resolver também problemas de segurança física e ambiental dos sistemas de rede e informação, incluindo, para tal, medidas para proteger estes sistemas contra falhas do sistema, erros humanos, ações maliciosas ou fenómenos naturais, em conformidade com as normas europeias e internacionais, como as que integram a série ISO/IEC 27000. A esse respeito, as entidades essenciais e importantes deverão, no quadro das suas medidas de gestão dos riscos de cibersegurança, atender também à segurança dos recursos humanos e dispor de políticas adequadas de controlo do acesso. Estas medidas deverão ser coerentes com a Diretiva (UE) 2022/2557.

(80) Para efeitos de demonstração do cumprimento das medidas de gestão dos riscos de cibersegurança e na ausência de sistemas europeus de certificação da cibersegurança adequados, adotados nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([18]), os Estados-Membros deverão, em consulta com o grupo de cooperação e do grupo europeu para a certificação da cibersegurança, promover a utilização de normas europeias e internacionais pertinentes pelas entidades essenciais e importantes ou poderão exigir que as entidades utilizem produtos de TIC, serviços de TIC e processos de TIC certificados.

(81) Para evitar impor encargos financeiros e administrativos desproporcionados às entidades essenciais e importantes, as medidas estabelecidas em matéria de gestão dos riscos de cibersegurança deverão ser proporcionadas em relação aos riscos para os sistemas de rede e informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas e, se aplicável, as normas europeias e internacionais pertinentes, bem como os custos relativos à sua aplicação.

(82) As medidas de gestão dos riscos de cibersegurança deverão ser proporcionais ao grau de exposição da entidade essencial ou importante aos riscos e ao impacto societal e económico que um incidente teria. Aquando do estabelecimento de medidas de gestão dos riscos de cibersegurança adaptadas às entidades essenciais e importantes, importa ter em devida conta os diferentes níveis de exposição aos riscos das entidades essenciais e importantes, tais como o caráter crítico da entidade, os riscos, incluindo os riscos societais, a que está exposta, a dimensão da entidade e a probabilidade de ocorrência de incidentes e respetiva gravidade, incluindo o seu impacto societal e económico.

([18]) 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).

(83) As entidades essenciais e importantes deverão garantir a segurança dos sistemas de rede e informação que utilizam nas suas atividades. Esses sistemas são constituídos principalmente por sistemas de rede e informação privados geridos por pessoal interno especializado em TI das entidades essenciais e importantes ou cuja segurança tenha sido externalizada. As medidas de gestão dos riscos de cibersegurança e as obrigações de notificação estabelecidos na presente diretiva deverão aplicar-se às entidades essenciais e importantes abrangidas, independentemente de a manutenção dos sistemas de rede e informação dessas entidades ser realizada a nível interno ou ser externalizada.

(84) Tendo em conta a sua natureza transfronteiriça, os prestadores de serviços de DNS, os registos de nomes de TLD, 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, os prestadores de serviços de segurança geridos, os prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais e os prestadores de serviços de confiança deverão estar sujeitos a um maior grau de harmonização a nível da União. A aplicação de medidas de gestão dos riscos de cibersegurança no que respeita a essas entidades deverá, por conseguinte, ser facilitada por um ato de execução.

(85) 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 dos sistemas de rede e informação de uma entidade mediante a exploração de vulnerabilidades que afetam produtos e serviços de terceiros, é particularmente importante gerir os riscos decorrentes da cadeia de abastecimento de uma entidade e da relação desta com os seus fornecedores, como os prestadores de serviços de armazenamento e tratamento de dados ou os prestadores de serviços de segurança geridos e os editores de software. Por conseguinte, as entidades essenciais e importantes deverão avaliar e ter em conta a qualidade e a resiliência globais dos produtos e serviços, as medidas de gestão dos riscos de cibersegurança neles integradas e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro. As entidades essenciais e importantes deverão, em particular, ser incentivadas a incorporar medidas de gestão dos riscos de cibersegurança nos acordos contratuais com os seus fornecedores e prestadores de serviços diretos. Essas entidades podem tomar em consideração os riscos decorrentes de outros níveis de fornecedores e prestadores de serviços.

(86) 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 evitar e detetar os incidentes, bem como para lhes dar resposta ou recuperar dos mesmos. Porém, os próprios prestadores de serviços de segurança geridos têm sido igualmente alvo de ciberataques e, em virtude da sua estreita integração nas atividades das entidades, representam um risco especial. As entidades essenciais e importantes deverão, assim, exercer uma diligência acrescida ao selecionarem um prestador de serviços de segurança geridos.

(87) As autoridades 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.

(88) As entidades essenciais e importantes deverão igualmente gerir os riscos emergentes da sua interação e da sua relação com outras partes interessadas no seio de um ecossistema mais vasto, nomeadamente no que se refere à luta contra a espionagem industrial e à proteção de segredos comerciais. Mais concretamente, essas 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 essenciais e importantes, quando recorrerem a serviços de transformação de dados e de análise de dados prestados por terceiros, essas entidades deverão tomar todas as medidas de gestão dos riscos de cibersegurança adequadas.

(89) As entidades essenciais e importantes deverão adotar uma vasta gama de práticas básicas de ciber-higiene, como princípios de «confiança zero», a atualização do software, a configuração dos dispositivos, a segmentação da rede, a gestão da identidade e do acesso ou a sensibilização dos utilizadores, organizar formações para o seu pessoal e aumentar a sensibilização para as ciberameaças, a mistificação da interface («*phishing*») ou as técnicas de engenharia social. Além disso, essas entidades deverão avaliar as suas próprias capacidades de cibersegurança e, se for caso disso, procurar a integração de tecnologias que reforcem a cibersegurança, como a inteligência artificial ou os sistemas de aprendizagem automática para melhorar as suas capacidades e a segurança dos sistemas de rede e informação.

(90) A fim de melhorar a gestão dos principais riscos da cadeia de abastecimento e de ajudar as entidades essenciais e importantes que atuam em setores abrangidos pela presente diretiva a gerirem adequadamente riscos relacionados com a cadeia de abastecimento e os fornecedores, o grupo de cooperação, em cooperação com a Comissão e a ENISA e, se for caso disso, após consulta das partes interessadas pertinentes, nomeadamente da indústria, deverá realizar avaliações coordenadas dos riscos de segurança associados às cadeias de abastecimento críticas, tal como foi já feito para as redes 5G na sequência da Recomendação (UE) 2019/534 da Comissão ([19]), com o objetivo de identificar, em cada setor, os produtos de TIC, sistemas de TIC ou serviços de TIC críticos, bem como as vulnerabilidades e ameaças importantes. Essas avaliações coordenadas dos riscos de segurança deverão identificar medidas, planos de atenuação e boas práticas para combater dependências críticas, potenciais falhas pontuais, ameaças, vulnerabilidades e outros riscos associados à cadeia de abastecimento e deverão explorar formas de incentivar a sua adoção mais generalizada pelas entidades essenciais e importantes. Os potenciais fatores de risco não-técnicos, como a influência indevida de um país terceiro nos fornecedores e nos prestadores de serviços, em particular no caso de modelos alternativos de governação, incluem vulnerabilidades ou acessos ocultos e potenciais perturbações sistémicas no abastecimento, em particular no caso de vinculação tecnológica ou de dependência dos fornecedores.

(91) Dadas as características do setor em causa, as avaliações coordenadas dos riscos de segurança associados às cadeias de abastecimento críticas 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 cibersegurança 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 abastecimento que deverão estar sujeitas a uma avaliação coordenada dos riscos de segurança, importa ter em conta os seguintes critérios: i) em que medida as entidades essenciais e importantes utilizam e dependem de produtos de TIC, sistemas de TIC ou serviços de TIC críticos específicos; ii) a importância de produtos de TIC, sistemas de TIC 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 de TIC, sistemas de TIC ou serviços de TIC alternativos; iv) a resiliência da cadeia global de abastecimento de produtos de TIC, sistemas de TIC ou serviços de TIC, ao longo do seu ciclo de vida, face a perturbações; e v) no que respeita a produtos de TIC, sistemas de TIC ou serviços de TIC emergentes, a sua potencial importância futura para as atividades das entidades. Além disso, deverá ser prestada especial atenção aos serviços de TIC, sistemas de TIC ou produtos de TIC sujeitos a requisitos específicos decorrentes de países terceiros.

(92) A fim de simplificar as obrigações 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 dos respetivos sistemas de rede e informação, bem como para permitir que essas entidades e as autoridades competentes nos termos da Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho ([20]) e do Regulamento (UE) n.º 910/2014, respetivamente, beneficiem do quadro jurídico estabelecido pela presente diretiva, incluindo a designação de uma CSIRT responsável pelo tratamento de incidentes e a participação das autoridades competentes em causa no trabalho do grupo de cooperação e da rede de CSIRT, as referidas entidades deverão estar abrangidas pelo âmbito de aplicação da presente diretiva. Por conseguinte, é necessário suprimir as correspondentes disposições do Regulamento (UE) n.º 910/2014 e da Diretiva (UE) 2018/1972 relacionadas com a imposição de obrigações em matéria de segurança e notificação a estes tipos de entidades. As regras em matéria de obrigações de notificação estabelecidas na presente diretiva deverão ser aplicáveis sem prejuízo das disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE.

(93) As obrigações em matéria de cibersegurança 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. 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 nos termos da presente diretiva. Tais obrigações em matéria de cibersegurança e de notificação deverão também dizer respeito à proteção física dos serviços prestados. Os requisitos aplicáveis aos prestadores de serviços de confiança qualificados previstos no artigo 24.º do Regulamento (UE) n.º 910/2014 continuam a ser aplicáveis.

([19]) 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).

([20]) 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).

(94) Os Estados-Membros podem atribuir as funções de autoridade competente pelos serviços de confiança aos organismos supervisores nos termos do Regulamento (UE) n.º 910/2014, a fim de assegurar a continuidade das práticas atuais e tirar partido dos conhecimentos e da experiência resultantes da aplicação do referido Regulamento. Nesse caso, as autoridades competentes nos termos da presente diretiva deverão cooperar estreitamente e em tempo útil, com esses organismos supervisores, trocando informações relevantes, a fim de assegurar uma supervisão eficaz e o cumprimento dos requisitos estabelecidos na presente diretiva e no Regulamento (UE) n.º 910/2014 pelos prestadores de serviços de confiança. Quando aplicável, a CSIRT ou a autoridade competente nos termos da presente diretiva deverá informar de imediato o organismo supervisor nos termos do Regulamento (UE) n.º 910/2014 de qualquer incidente ou ciberameaça significativa notificados que afetem os serviços de confiança, bem como de qualquer infração à presente diretiva por parte dos prestadores de serviços de confiança. Para efeitos de notificação, os Estados-Membros podem, se aplicável, recorrer ao ponto de entrada único estabelecido para efetuar a notificação comum e automática de incidentes tanto ao organismo supervisor nos termos do Regulamento (UE) n.º 910/2014, como à CSIRT ou à autoridade competente nos termos da presente diretiva.

(95) Quando for caso disso e para evitar perturbações desnecessárias, as orientações nacionais em vigor adotadas para efeitos de transposição das regras relacionadas com medidas de segurança estabelecidas nos artigos 40.º e 41.º da Diretiva (UE) 2018/1972 deverão ser tidas em conta na transposição da presente diretiva, tendo, assim, por base os conhecimentos e as competências resultantes da aplicação da Diretiva (UE) 2018/1972 no que se refere às medidas de segurança e à notificação de incidentes. A ENISA pode também elaborar orientações para os requisitos em matéria de segurança e para as obrigações de notificação destinados aos fornecedores de redes públicas de comunicações eletrónicas 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 ao abrigo da Diretiva (UE) 2018/1972, a fim de assegurar a continuidade das práticas atuais e tirar partido dos conhecimentos e da experiência resultantes da aplicação dessa diretiva.

(96) Dada a importância crescente dos serviços de comunicações interpessoais independentes do número, na aceção da Diretiva (UE) 2018/1972, é necessário assegurar que tais serviços também estejam sujeitos a requisitos de segurança adequados, tendo em conta a sua natureza específica e importância económica. À medida que a superfície de ataque continua a expandir-se, os serviços de comunicações interpessoais independentes do número, como os serviços de mensagens, estão a tornar-se vetores de ataque generalizados. Os intervenientes maliciosos utilizam plataformas para comunicar e levar as vítimas a abrir páginas Web expostas, aumentando assim a probabilidade de incidentes que envolvam a exploração de dados pessoais e, por extensão, a segurança dos sistemas de rede e informação. Assim, os prestadores de serviços de comunicações interpessoais independentes do número deverão garantir um nível de segurança dos sistemas de rede e 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 para esses 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, na aceção da Diretiva (UE) 2018/1972, que utilizam números e que não exercem um controlo efetivo sobre a transmissão de sinais.

(97) O mercado interno depende, mais do que nunca, do funcionamento da Internet. Os serviços de quase 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 todos os fornecedores de redes públicas de comunicações eletrónicas adotem medidas de gestão dos riscos de cibersegurança adequadas e notifiquem incidentes significativos relacionados com as mesmas. Os Estados-Membros deverão assegurar a manutenção da segurança das redes públicas de comunicações eletrónicas e a proteção dos seus interesses vitais em matéria de segurança contra sabotagem e espionagem. Uma vez que a conectividade internacional reforça e acelera a digitalização competitiva da União e da sua economia, os incidentes que afetam os cabos submarinos de comunicações deverão ser notificados à CSIRT ou, se aplicável, à autoridade competente. A estratégia nacional de cibersegurança deverá, quando pertinente, ter em conta a cibersegurança dos cabos submarinos de comunicações e incluir um levantamento dos potenciais riscos de cibersegurança e medidas de atenuação para garantir o mais elevado nível de proteção dos mesmos.

(98) Para salvaguardar a segurança das redes públicas de comunicações eletrónicas e dos serviços de comunicações eletrónicas acessíveis ao público, deverá ser promovida a utilização de tecnologias de cifragem, especialmente da cifragem de ponta a ponta, bem como de conceitos de segurança centrados nos dados, como a cartografia, a segmentação, a etiquetagem, uma política de acesso e a gestão do acesso, bem como decisões de acesso automatizadas. Se necessário, a utilização de cifragem, em particular de cifragem de ponta a ponta, deverá ser obrigatória para os fornecedores de redes públicas de comunicações eletrónicas ou os prestadores de serviços de comunicações eletrónicas acessíveis ao público, em conformidade com os princípios da segurança e da privacidade por defeito e desde a conceção para efeitos da presente diretiva. 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 prevenção, a investigação, a deteção e a repressão de infrações penais em conformidade com o direito da União. No entanto, tal não deverá enfraquecer a cifragem de ponta a ponta, que é uma tecnologia fundamental para uma proteção eficaz dos dados, da privacidade e da segurança das comunicações.

(99) Para salvaguardar a segurança e prevenir abusos e a manipulação das redes públicas de comunicações eletrónicas e dos serviços de comunicações eletrónicas acessíveis ao público, deverá ser promovida a utilização de normas de encaminhamento seguro, a fim de garantir a integridade e a robustez das funções de encaminhamento em todo o ecossistema de prestadores de serviços de acesso à Internet.

(100) Para salvaguardar a funcionalidade e a integridade da Internet e promover a segurança e a resiliência do DNS, as partes interessadas pertinentes, nomeadamente as entidades do setor privado da União, os prestadores de serviços de comunicações eletrónicas acessíveis ao público, em particular os prestadores de serviços de acesso à Internet, bem como os fornecedores de motores de pesquisa em linha deverão ser incentivados a adotar uma estratégia de diversificação da resolução do DNS. Além disso, os Estados-Membros deverão incentivar o desenvolvimento e a utilização de um serviço europeu, público e seguro de resolução do DNS.

(101) A presente diretiva define uma abordagem em várias etapas à notificação de incidentes significativos, a fim de estabelecer o equilíbrio adequado entre, por um lado, uma notificação célere que ajude a minimizar a potencial propagação de incidentes significativos e permita às entidades essenciais e importantes procurar assistência e, por outro lado, uma notificação exaustiva que retire ensinamentos valiosos de incidentes individuais e melhore gradualmente a ciber-resiliência de empresas individuais e setores inteiros. Neste contexto, a presente diretiva deverá incluir a notificação de incidentes que, com base numa avaliação inicial realizada pela entidade em causa, possam causar perturbações operacionais ou perdas financeiras graves a essa entidade ou afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis. Esta avaliação inicial deverá ter em conta, nomeadamente, os sistemas de rede e informação afetados e, em particular, a sua importância para a prestação dos serviços da entidade, a gravidade e as características técnicas da ciberameaça e quaisquer vulnerabilidades subjacentes alvo de exploração, bem como a experiência da entidade com incidentes semelhantes. Indicadores como a medida em que o funcionamento do serviço é afetado, a duração de um incidente ou o número de destinatários de serviços afetados podem desempenhar um papel importante para determinar se a perturbação operacional do serviço é grave.

(102) Quando tenham tido conhecimento de um incidente significativo, as entidades essenciais e importantes deverão ser obrigadas a enviar um alerta rápido sem demora injustificada e, em qualquer caso, no prazo de 24 horas. Esse alerta rápido deverá ser seguido de uma notificação de incidente. As entidades em causa deverão enviar uma notificação de incidente sem demora injustificada e, em qualquer caso, no prazo de 72 horas depois de terem tomado conhecimento do incidente significativo, com o objetivo, nomeadamente, de atualizar as informações transmitidas no âmbito do alerta rápido e de fornecer uma avaliação inicial do incidente significativo, incluindo da sua gravidade e do seu impacto, bem como indicadores de exposição a riscos, se disponíveis. O mais tardar um mês após a notificação de incidente, deverá ser apresentado um relatório final. O alerta rápido deverá conter apenas as informações necessárias para dar conhecimento do incidente significativo à CSIRT, ou à autoridade competente se aplicável, e para permitir que a entidade em causa procure assistência, caso tal seja necessário. Esse alerta rápido deve, se aplicável, indicar se existem suspeitas de que o incidente significativo foi provocado por atos ilícitos ou maliciosos e se é suscetível de ter um impacto transfronteiriço. Os Estados-Membros deverão garantir que a obrigação de apresentar o alerta rápido, ou a subsequente notificação de incidente, não desvie os recursos da entidade notificadora afetos a atividades relacionadas com o tratamento de incidentes, às quais deverá ser atribuída prioridade, a fim de evitar que as obrigações de notificação de incidentes desviem recursos afetos à resposta a

incidentes significativos ou prejudiquem de qualquer outra forma os esforços envidados pelas entidades nessa matéria. Em caso de incidente em curso no momento da apresentação do relatório final, os Estados-Membros deverão assegurar que as entidades em causa apresentem um relatório intercalar nessa altura e um relatório final no prazo de um mês após terem resolvido o incidente significativo.

(103) Quando aplicável, as entidades essenciais e importantes deverão informar sem demora injustificada os destinatários dos seus serviços sobre quaisquer medidas ou soluções que podem adotar para minimizar os riscos resultantes de uma ciberameaça significativa. Se for caso disso e em particular quando a ciberameaça significativa for suscetível de se concretizar, essas entidades deverão informar também os destinatários dos seus serviços sobre a ameaça em causa. A exigência de informar os referidos destinatários das ciberameaças significativas deverá ser cumprida na medida do possível, mas não deverá isentar essas entidades da obrigação de, a expensas suas, adotarem medidas adequadas e imediatas para prevenir ou remediar quaisquer ameaças e restabelecer o nível normal de segurança do serviço. A prestação dessas informações aos destinatários dos serviços sobre ciberameaças significativas deverá ser gratuita e feita numa linguagem facilmente compreensível.

(104) Os fornecedores de redes públicas de comunicações eletrónicas ou os prestadores de serviços de comunicações eletrónicas acessíveis ao público deverão implementar a segurança desde a conceção e por defeito e informar os destinatários dos serviços sobre ciberameaças significativas e sobre as medidas que podem tomar para proteger a segurança dos seus dispositivos e das suas comunicações, por exemplo, recorrendo a tipos específicos de software ou tecnologias de cifragem.

(105) Uma abordagem proativa das ciberameaças é uma componente vital das medidas de gestão dos riscos de cibersegurança que deverá dar às autoridades competentes condições para impedirem eficazmente que as ciberameaças se transformem em incidentes suscetíveis de causar danos materiais ou imateriais consideráveis. Para o efeito, reveste-se de uma importância fundamental a notificação de ciberameaças. As entidades são, por conseguinte, incentivadas a notificar a título voluntário as ciberameaças.

(106) A fim de simplificar a comunicação das informações exigidas pela presente diretiva, bem como de reduzir os encargos administrativos para as entidades, os Estados-Membros deverão disponibilizar meios técnicos, como um ponto de entrada único, sistemas automatizados, formulários em linha, interfaces de fácil utilização, modelos e plataformas específicas para utilização pelas entidades, independentemente de serem abrangidas ou não pelo âmbito de aplicação da presente diretiva, para a apresentação das informações pertinentes a notificar. O financiamento da União destinado a apoiar a aplicação da presente diretiva, em particular no âmbito do Programa Europa Digital criado pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho ([21]), pode incluir o apoio a pontos de entrada únicos. Ademais, as entidades 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 administrativos adicionais, podendo igualmente gerar dúvidas quanto ao formato e aos procedimentos aplicáveis a tais notificações. Sempre que seja estabelecido um ponto de entrada único, os Estados-Membros são também incentivados a recorrer a esse ponto de entrada único para as notificações de incidentes de segurança exigidas por outros instrumentos do direito da União, como o Regulamento (UE) 2016/679 e a Diretiva 2002/58/ /CE. A utilização desse ponto de entrada único para a notificação de incidentes de segurança nos termos do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE não deverá afetar a aplicação das disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE, em particular as relativas à independência das autoridades aí referidas. A ENISA, em colaboração com o grupo de cooperação, deverá criar modelos comuns de notificação por intermédio de orientações destinadas a simplificar e racionalizar a comunicação das informações a notificar nos termos do direito da União e a reduzir os encargos administrativos sobre as entidades notificadoras.

(107) Os Estados-Membros deverão 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. Se for caso disso, 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.

([21]) Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240 (JO L 166 de 11.5.2021, p. 1).

(108) Os dados pessoais ficam amiúde expostos em consequência de incidentes. Nesse contexto, as entidades competentes deverão cooperar e trocar informações sobre todas as questões pertinentes com as autoridades referidas no Regulamento (UE) 2016/679 e na Diretiva 2002/58/CE.

(109) A manutenção de bases de dados fidedignas e completas dos dados relativos ao registo de nomes de domínio («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 em toda a União. Para esse efeito específico, os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão ser obrigados a tratar determinados dados necessários para alcançar esse objetivo. Esse tratamento deverá constituir uma obrigação jurídica na aceção do artigo 6.º, n.º 1, alínea c), do Regulamento (UE) 2016/679. Essa obrigação aplica-se sem prejuízo da possibilidade de recolher dados relativos ao registo de nomes de domínio para outros fins, por exemplo, com base em disposições contratuais ou requisitos legais estabelecidos noutros instrumentos do direito da União ou do direito nacional. Essa obrigação visa alcançar um conjunto completo e exato de dados de registo e não deverá dar origem à recolha repetida dos mesmos dados. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão cooperar entre si, a fim de evitar a duplicação dessa tarefa.

(110) A disponibilização e a concessão atempada dos dados relativos ao registo de nomes de domínio aos requerentes legítimos de acesso são fundamentais para prevenir e combater os abusos dos DNS, bem como para prevenir e detetar incidentes e para lhes dar resposta. Os requerentes legítimos de acesso devem ser entendidos como qualquer pessoa singular ou coletiva que apresente um pedido nos termos do direito da União ou do direito nacional. Podem incluir as autoridades competentes nos termos da presente diretiva e as que são competentes nos termos do direito da União ou do direito nacional para a prevenção, investigação, deteção ou repressão de infrações penais, e CERT ou CSIRT. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão permitir o acesso lícito a dados específicos de registo de nomes de domínio, que são necessários para efeitos do pedido de acesso, aos requerentes legítimos de acesso, em conformidade com o direito da União e o direito nacional. O pedido dos requerentes legítimos de acesso deverá ser acompanhado de uma exposição de motivos que permita avaliar a necessidade de acesso aos dados.

(111) A fim de assegurar a disponibilidade de dados exatos e completos relativos ao registo de nomes de domínio, os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão recolher dados relativos ao registo de nomes de domínio e garantir a integridade e disponibilidade desses dados. Em especial, os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão estabelecer políticas e procedimentos para recolher e manter dados exatos e completos relativos ao registo de nomes de domínio, bem como para evitar e corrigir dados de registo incorretos, em conformidade com o direito da União em matéria de proteção de dados. Essas políticas e procedimentos deverão ter em conta, na medida do possível, as normas elaboradas pelas estruturas de governação multilateral a nível internacional. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão adotar e aplicar procedimentos proporcionados de verificação dos dados relativos ao registo de nomes de domínio. Esses procedimentos deverão refletir as melhores práticas utilizadas no setor e, na medida do possível, os progressos realizados no domínio da identificação eletrónica. Os exemplos de procedimentos de verificação podem incluir controlos *ex ante* realizados no momento do registo e controlos *ex post* realizados após o registo. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão, em particular, verificar pelo menos um meio de contacto do requerente do registo.

(112) Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão ser obrigadas a disponibilizar ao público dados relativos ao registo de nomes de domínio que não estejam abrangidos pelo âmbito de aplicação do direito da União em matéria de proteção de dados, como os dados respeitantes a pessoas coletivas, em conformidade com o preâmbulo do Regulamento (UE) 2016/679. No caso das pessoas coletivas, os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão disponibilizar ao público, pelo menos, o nome do requerente do registo e o número de telefone de contacto. O endereço eletrónico de contacto deverá também ser publicado, desde que não contenha quaisquer dados pessoais, nomeadamente quando são usados pseudónimos de correio eletrónico ou contas funcionais. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão 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 o direito da União em matéria de proteção de dados. Os Estados-Membros deverão exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio 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. Os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio deverão 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. Essas políticas e procedimentos deverão ter em conta, na medida do possível, quaisquer orientações e as normas elaboradas pelas estruturas de governação multilateral a nível internacional. O procedimento de acesso pode contemplar a utilização de uma interface, de um portal ou de outra ferramenta técnica para disponibilizar um sistema eficiente de pedido e acesso a dados de registo. A fim de promover práticas harmonizadas em todo o mercado interno, a Comissão pode, sem prejuízo das competências do Comité Europeu para a Proteção de Dados, fornecer orientações sobre tais procedimentos, que tenham em conta, na medida do possível, as normas elaboradas pelas estruturas de governação multilateral a nível internacional. Os Estados-Membros deverão assegurar que todos os tipos de acesso aos dados pessoais e não pessoais de registo de nomes de domínio sejam gratuitos.

(113) As entidades abrangidas pelo âmbito de aplicação da presente diretiva deverão estar sob a jurisdição do Estado-Membro em que se encontram estabelecidas. No entanto, os fornecedores de redes públicas de comunicações eletrónicas ou os prestadores de serviços de comunicações eletrónicas acessíveis ao público deverão ser considerados como estando sob a jurisdição do Estado-Membro em que prestam os seus serviços. Os prestadores de serviços de DNS, os registos de nomes de TLD, as entidades que prestam serviços de registo de nomes de domínio, 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, os prestadores de serviços de segurança geridos, bem como os prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, deverão ser considerados como estando sob a jurisdição do Estado-Membro em que têm o seu estabelecimento principal na União. As entidades da administração pública deverão estar sob a jurisdição do Estado-Membro que as estabeleceu. Se uma entidade prestar serviços ou estiver estabelecida em mais do que um Estado-Membro, deverá estar sob a jurisdição autónoma e concorrente de cada um desses Estados-Membros. As autoridades competentes desses Estados-Membros deverão cooperar, prestar assistência mútua e, se for caso disso, realizar ações de supervisão conjuntas. Sempre que os Estados-Membros exerçam jurisdição, não deverão aplicar medidas de execução nem sanções mais do que uma vez pelo mesmo comportamento, em conformidade com o princípio *ne bis in idem*.

(114) Para ter em conta a natureza transfronteiriça dos serviços e operações dos prestadores de serviços de DNS, dos registos de nomes de TLD, das entidades que prestam serviços de registo de nomes de domínio, dos prestadores de serviços de computação em nuvem, dos prestadores de serviços de centro de dados, dos fornecedores de redes de distribuição de conteúdos, dos prestadores de serviços geridos, dos prestadores de serviços de segurança geridos bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, estas entidades deverão estar sob a jurisdição de um único Estado-Membro. A competência deverá ser atribuída ao Estado-Membro onde a entidade em causa 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 desse critério não deverá estar subordinado à presença física dos sistemas de rede e 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 deverá ser considerado como tendo lugar no Estado-Membro 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 não for possível determinar esse Estado-Membro ou se tais decisões não forem tomadas na União, deverá considerar-se que o estabelecimento principal se situa no Estado-Membro em que são levadas a cabo as operações de cibersegurança. Se não for possível determinar esse Estado-Membro, 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.

(115) Quando um serviço de DNS recursivo disponível ao público 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.

(116) Sempre que ofereça serviços na União, um prestador de serviços de DNS, um registo de nomes de TLD, uma entidade que presta serviços de registo de nomes de domínio, um prestador de serviços de computação em nuvem, um prestador de serviços de centro de dados, um fornecedor de redes de distribuição de conteúdos, um prestador de serviços geridos, um prestador de serviços de segurança geridos ou um prestador de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais que não esteja estabelecido na União deverá designar um representante na União. A fim de determinar se tal entidade oferece serviços na União, há que apurar se tem a 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 deverá ser considerado insuficiente 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 língua, ou a referência a clientes ou utilizadores na União são suscetíveis de revelar que a entidade tenciona oferecer serviços na União. O representante deverá atuar por conta da entidade e as autoridades competentes ou as CSIRT deverão poder dirigir-se a ele. O representante deverá 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.

(117) A fim de assegurar uma visão de conjunto clara dos prestadores de serviços de DNS, dos registos de nomes de TLD, das entidades que prestam serviços de registo de nomes de domínio, dos prestadores de serviços de computação em nuvem, dos prestadores de serviços de centro de dados, dos fornecedores de redes de distribuição de conteúdos, dos prestadores de serviços geridos, dos prestadores de serviços de segurança geridos, bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais que prestam, em toda a União, serviços abrangidos pelo âmbito de aplicação da presente diretiva, a ENISA deverá criar e manter um registo dessas entidades, com base nas informações recebidas pelos Estados-Membros, se aplicável através de mecanismos nacionais estabelecidos para se registarem a si mesmas. Os pontos de contacto únicos deverão transmitir à ENISA as informações e quaisquer alterações às mesmas. Com o intuito de garantir a exatidão e a exaustividade das informações a incluir no referido registo, os Estados-Membros podem apresentar à ENISA as informações disponíveis nos registos nacionais a respeito dessas entidades. A ENISA e os Estados-Membros deverão tomar medidas para facilitar a interoperabilidade desses registos, assegurando simultaneamente a proteção das informações confidenciais ou classificadas. A ENISA deverá estabelecer protocolos adequados de classificação e gestão da informação, de molde a garantir a segurança e a confidencialidade das informações divulgadas e a restringir o acesso, o armazenamento e a transmissão dessas informações aos utilizadores a que se destinam.

(118) Se, ao abrigo da presente diretiva, forem trocadas, comunicadas ou de outro modo partilhadas informações classificadas em conformidade com o direito da União ou o direito nacional, deverão ser aplicadas as regras correspondentes sobre o tratamento de informações classificadas. Além disso, a ENISA deverá dispor das infraestruturas, dos procedimentos e das regras necessárias para o tratamento de informações sensíveis e classificadas, em conformidade com as regras de segurança aplicáveis à proteção das informações classificadas da UE.

(119) Dado que as ciberameaças têm vindo a tornar-se mais complexas e sofisticadas, a deteção eficaz de tais ameaças e as medidas para as prevenir dependem, em grande medida, da troca regular, entre as entidades, de informações sobre ameaças e vulnerabilidades. 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 tais ameaças se materializem sob a forma de 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.

(120) As entidades deverão ser incentivadas e assistidas pelos Estados-Membros no sentido de, coletivamente, tirarem partido dos seus conhecimentos e experiências práticas individuais a nível estratégico, tático e operacional, tendo em vista o reforço das suas capacidades para, de forma adequada, prevenir e detetar incidentes, bem como para lhes dar resposta, para permitir a recuperação após estes incidentes e para atenuar o seu impacto. Consequentemente, é necessário permitir a emergência, a nível da União, de acordos de partilha de informações sobre cibersegurança de cariz voluntário. Para tal, os Estados-Membros deverão prestar assistência ativa e incentivar entidades, tais como as entidades que prestam serviços e fazem investigação no domínio da cibersegurança, bem como as entidades pertinentes não abrangidas pelo âmbito de aplicação da presente diretiva, a participarem em tais acordos de partilha de informações sobre cibersegurança. Esses acordos deverão ser estabelecidos em conformidade com as regras da União em matéria de concorrência e de proteção de dados.

(121) O tratamento de dados pessoais, efetuado na medida estritamente necessária e proporcionada para assegurar a segurança dos sistemas de rede e informação, por entidades essenciais e importantes poderá ser considerado lícito pelo facto de respeitar uma obrigação jurídica a que o responsável pelo tratamento está sujeito, em conformidade com os requisitos estabelecidos pelo artigo 6.º, n.º 1, alínea c), e pelo artigo 6.º, n.º 3, do Regulamento (UE) 2016/679. O tratamento de dados pessoais pode também ser necessário para efeito dos interesses legítimos prosseguidos por entidades essenciais e importantes, bem como por fornecedores de tecnologias e prestadores de serviços de segurança que atuem em nome dessas entidades, nos termos do artigo 6.º, n.º 1, alínea f), do Regulamento (UE) 2016/679, nomeadamente quando tal tratamento é necessário aos acordos de partilha de informações sobre cibersegurança ou à notificação voluntária de informações pertinentes em conformidade com a presente diretiva. Medidas relacionadas com a prevenção, deteção, identificação, contenção, 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 poderão implicar o tratamento de determinadas categorias de dados pessoais, tais como endereços IP, localizadores uniformes de recursos (URL), nomes de domínio, endereços de correio eletrónico, e, sempre que revelem dados pessoais, selos temporais. O tratamento de dados pessoais pelas autoridades competentes, pelos pontos de contacto únicos e pelas CSIRT pode constituir uma obrigação jurídica ou ser considerado necessário para o exercício de uma missão de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento, nos termos do artigo 6.º, n.º 1, alíneas c) ou e), e do artigo 6.º, n.º 3, do Regulamento (UE) 2016/679, ou para a prossecução de um interesse legítimo das entidades essenciais e importantes, tal como referido no artigo 6.º, n.º 1, alínea f), do referido regulamento. Além disso, é possível que o direito nacional estabeleça regras que — na medida do necessário e proporcionado para garantir a segurança dos sistemas de rede e informação de entidades essenciais e importantes — permitam às autoridades competentes, aos balcões únicos e às CSIRT tratar categorias específicas de dados pessoais em conformidade com o artigo 9.º do Regulamento (UE) 2016/679, mormente prevendo medidas adequadas e específicas para salvaguardar os direitos e interesses fundamentais das pessoas singulares, nomeadamente restrições técnicas no que diz respeito à reutilização desses dados e o recurso às medidas tecnologicamente mais avançadas em matéria de segurança e de preservação da privacidade, como a pseudonimização ou a cifragem, sempre que a anonimização possa afetar significativamente a finalidade prosseguida.

(122) 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 deverá 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 essas 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 das medidas de gestão dos riscos de cibersegurança e que as autoridades competentes deverão adotar uma abordagem *ex post* reativa à supervisão, pelo que não estão sujeitas a uma obrigação geral de supervisionar essas entidades. A supervisão *ex post* das entidades importantes pode ser desencadeada por elementos de prova, indicações ou informações levadas ao conhecimento das autoridades competentes que estas considerem sugerir potenciais infrações à presente diretiva. Por exemplo, esses elementos de prova, indicações ou informações poderão ser do tipo transmitido às autoridades competentes por outras autoridades, entidades, cidadãos, meios de comunicação social ou outras fontes, ou informações acessíveis ao público, ou poderão resultar de outras atividades realizadas pelas autoridades competentes no exercício das suas funções.

(123) O desempenho das funções de supervisão pelas autoridades competentes não deverá dificultar desnecessariamente as atividades comerciais da entidade em causa. Sempre que desempenhem as suas funções de supervisão em relação a entidades essenciais – nomeadamente procedendo à realização de inspeções no local e à supervisão fora do local, à investigação de infrações à presente diretiva, ou à realização de auditorias ou de verificações de segurança –, as autoridades competentes deverão minimizar o impacto nas atividades empresariais da entidade em causa.

(124) Quando exercem uma supervisão *ex ante*, as autoridades competentes deverão estar aptas a definir prioridades no que diz respeito ao recurso proporcionado às medidas e meios de supervisão de que dispõem. Tal significa que as autoridades competentes podem definir essas 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 medidas 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 poderiam também ser

acompanhadas de programas de trabalho e ser avaliadas e revistas com regularidade, nomeadamente quanto a aspetos como a afetação de recursos e as necessidades em termos de recursos. Em relação às entidades da administração pública, as competências de supervisão deverão ser exercidas em conformidade com os quadros legislativos e institucionais nacionais.

(125) As autoridades competentes deverão assegurar que as suas funções de supervisão no que diz respeito às entidades essenciais e importantes são desempenhadas por profissionais formados, com as competências necessárias para levar a cabo as tarefas em causa, em especial no que diz respeito à realização de inspeções no local e à supervisão fora do local, nomeadamente a identificação de deficiências em matéria de bases de dados, equipamento informático, barreiras de proteção, encriptação e redes. Essas inspeções e a supervisão em causa deverão ser realizadas de forma objetiva.

(126) Nos casos devidamente fundamentados em que tenha conhecimento de uma ciberameaça significativa ou de um risco iminente, a autoridade competente deverá poder tomar decisões de execução imediatas com o objetivo de prevenir ou de dar resposta a um incidente.

(127) Para que a execução seja eficaz, há que estabelecer uma lista mínima de poderes de execução que podem ser aplicados em caso de incumprimento das medidas de gestão dos riscos de cibersegurança e das obrigações de notificação previstas na presente diretiva, definindo um quadro claro e consistente para tal execução em toda a União. Importa ter em devida conta a natureza, a gravidade e a duração da infração à presente diretiva, os danos materiais ou imateriais causados, se a infração foi de caráter intencional ou negligente, as medidas tomadas para prevenir ou atenuar os danos materiais ou imateriais, o grau de responsabilidade ou quaisquer infrações anteriores pertinentes, o grau de cooperação com a autoridade competente e qualquer outra circunstância agravante ou atenuante. As medidas de execução, incluindo coimas, deverão ser proporcionadas e a sua imposição deverá 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 (a «Carta»), nomeadamente a tutela jurisdicional efetiva, o direito a um processo equitativo, a presunção de inocência e os direitos de defesa.

(128) A presente diretiva não impõe aos Estados-Membros a obrigação de preverem uma responsabilidade penal ou civil relativamente às pessoas singulares às quais incumbe assegurar que uma entidade cumpra o disposto na presente diretiva pelos danos sofridos por terceiros em resultado de uma infração à presente diretiva.

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

(130) Sempre que forem impostas coimas a uma entidade essencial ou importante que seja uma empresa, esta deverá, para esse efeito, ser entendida como sendo uma empresa na aceção dos artigos 101.º e 102.º do TFUE. Sempre que forem impostas coimas a pessoas que não sejam empresas, a autoridade competente deverá 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. Deverá 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 das autoridades competentes nem a aplicação de outras sanções estabelecidas nas regras nacionais que transpõem a presente diretiva.

(131) Os Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por infrações às regras nacionais que transpõem a presente diretiva. Contudo, a imposição de sanções penais por infrações às referidas regras nacionais e de sanções administrativas conexas não pode configurar uma violação do princípio *ne bis in idem*, tal como interpretado pelo Tribunal de Justiça da União Europeia.

(132) Sempre que a presente diretiva não harmonize sanções administrativas, ou se necessário noutros casos (por exemplo, em caso de infração grave à presente diretiva), os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. O direito nacional deverá estabelecer a natureza de tais sanções e se se trata de sanções penais ou administrativas.

(133) Com vista a reforçar a eficácia e o caráter dissuasivo das medidas de execução aplicáveis por infração à presente diretiva, as autoridades competentes deverão estar habilitadas a suspender temporariamente ou solicitar uma suspensão temporária de uma certificação ou autorização para a totalidade ou parte dos serviços pertinentes prestados por uma entidade essencial e solicitar a imposição de uma interdição temporária do exercício de funções de direção por uma pessoa singular a nível de diretor executivo ou de representante legal. Dada a sua severidade e o seu impacto nas atividades das entidades e, em última análise, nos seus clientes, tais suspensões ou proibições temporárias só deverão ser aplicadas de modo proporcional 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 materiais ou imateriais. Essas suspensões ou proibições temporárias só deverão ser aplicadas em último recurso, ou seja, apenas depois de esgotadas todas as outras medidas de execução pertinentes previstas na presente diretiva, e apenas até que as entidades em causa tenham tomado as medidas necessárias para corrigir as deficiências ou satisfazer os requisitos da autoridade competente que estiveram na origem da aplicação das suspensões ou proibições temporárias. A imposição de tais suspensões ou proibições temporárias deverá ser sujeita a garantias processuais adequadas, em conformidade com os princípios gerais do direito da União e da Carta, como o direito a um recurso efetivo e a um processo equitativo, a presunção de inocência e os direitos de defesa.

(134) A fim de assegurar que as entidades cumpram as obrigações que lhes incumbem por força da presente diretiva, os Estados-Membros deverão cooperar entre si e prestar assistência mútua no que diz respeito às medidas de supervisão e execução, em especial quando uma entidade presta serviços em mais do que um Estado-Membro ou quando os seus sistemas de rede e informação estão situados num Estado-Membro diferente daquele em que presta serviços. Ao prestar assistência, a autoridade competente requerida deverá tomar medidas de supervisão ou de execução em conformidade com o direito nacional. A fim de assegurar o bom funcionamento da assistência mútua nos termos da presente diretiva, as autoridades competentes deverão recorrer ao grupo de cooperação enquanto fórum para debater casos e pedidos específicos de assistência.

(135) A fim de assegurar uma supervisão e execução eficazes, nomeadamente quando a situação assume uma dimensão transfronteiriça, o Estado-Membro que tenha recebido um pedido de assistência mútua deverá, dentro dos limites desse pedido, tomar medidas de supervisão e execução adequadas em relação à entidade que é objeto desse pedido e que presta serviços ou que tem um sistema de rede e informação no território desse Estado-Membro.

(136) A presente diretiva deverá definir regras em matéria de cooperação entre as autoridades competentes e as autoridades de controlo, ao abrigo do Regulamento (UE) 2016/679, com vista ao tratamento de infrações à presente diretiva relacionadas com dados pessoais.

(137) A presente diretiva deverá procurar assegurar um elevado nível de responsabilidade pelas medidas de gestão dos riscos de cibersegurança e pelas obrigações de notificação ao nível das entidades essenciais e importantes. Por conseguinte, os órgãos de direção das entidades essenciais e importantes deverão aprovar as medidas de gestão dos riscos de cibersegurança e supervisionar a sua aplicação.

(138) A fim de garantir um elevado nível comum de cibersegurança em toda a União com base na presente diretiva, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão com vista a complementar a presente diretiva, especificando as categorias de entidades essenciais e importantes que devem ser obrigadas a utilizar determinados produtos, serviços e processos de TIC certificados ou a obter um certificado ao abrigo de um sistema europeu de certificação da cibersegurança. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([22]). Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

([22]) JO L 123 de 12.5.2016, p. 1.

(139) A fim de assegurar condições uniformes para a execução da presente diretiva, deverão ser atribuídas competências de execução à Comissão para estabelecer as disposições processuais necessárias ao funcionamento do grupo de cooperação e os requisitos técnicos, metodológicos e setoriais relativos às medidas de gestão dos riscos de cibersegurança, bem como para especificar mais pormenorizadamente o tipo de informações, o formato e o procedimento das notificações de incidentes, de ciberameaças e de quase incidentes e das comunicações relativas a ciberameaças significativas, bem como os casos em que um incidente deve ser considerado significativo. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([23]).

(140) A Comissão deverá avaliar regularmente a presente diretiva, em consulta com as partes interessadas, nomeadamente para decidir se é adequado propor alterações à luz da evolução das condições sociais, políticas, tecnológicas ou do mercado. No âmbito dessas avaliações, a Comissão deverá analisar a pertinência da dimensão das entidades em causa, dos setores, dos subsetores e dos tipos de entidades referidas nos anexos da presente diretiva para o funcionamento da economia e da sociedade no que diz respeito à cibersegurança. A Comissão deverá avaliar, nomeadamente, se os fornecedores abrangidos pelo escopo da presente diretiva que sejam classificados como plataformas em linha de muito grande dimensão na aceção do artigo 33.º do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho ([24]) podem ser identificadas como entidades essenciais nos termos da presente diretiva.

(141) A presente diretiva atribui novas tarefas à ENISA, reforçando assim o seu papel, o que poderá também fazer com que a ENISA tenha de desempenhar as atuais atribuições que lhe incumbem por força do Regulamento (UE) 2019/881 a um nível mais elevado do que anteriormente. A fim de assegurar que a ENISA disponha dos recursos financeiros e humanos necessários para realizar as atuais e as novas atribuições, bem como para satisfazer eventuais normas mais elevadas resultantes do seu papel reforçado, o seu orçamento deverá ser aumentado em conformidade. Além disso, com o intuito de garantir uma utilização eficiente dos recursos, a ENISA deverá dispor de maior flexibilidade na forma como pode afetar recursos a nível interno, de modo a poder desempenhar eficazmente as suas funções e ir ao encontro das expectativas.

(142) Atendendo a que o objetivo da presente diretiva, a saber, atingir um elevado nível comum de cibersegurança em toda a União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação, 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.

(143) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta, nomeadamente o direito ao respeito pela vida privada e pelo caráter privado das comunicações, o direito à proteção de dados pessoais, a liberdade de empresa, o direito de propriedade, o direito à ação e a um tribunal imparcial, a presunção de inocência e os direitos de defesa. O direito a um recurso efetivo estende-se aos destinatários dos serviços prestados por entidades essenciais e importantes. A presente diretiva deverá ser aplicada de acordo com esses direitos e princípios.

(144) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([25]) e emitiu parecer em 11 de março de 2021 ([26]),

---

([23]) 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).

([24]) Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO L 277 de 27.10.2022, p. 1).

([25]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

([26]) JO C 183 de 11.5.2021, p. 3.

ADOTARAM A PRESENTE DIRETIVA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

1. A presente diretiva estabelece medidas que visam a consecução de um elevado nível comum de cibersegurança na União, com vista a melhorar o funcionamento do mercado interno.

2. Para o efeito, a presente diretiva estabelece:

a) A obrigação de os Estados-Membros adotarem estratégias nacionais de cibersegurança e de designarem ou criarem autoridades competentes, autoridades de gestão de cibercrises, pontos de contacto únicos em matéria de cibersegurança (pontos de contacto únicos) e equipas de resposta a incidentes de segurança informática (CSIRT);

b) Medidas de gestão dos riscos de cibersegurança e obrigações de notificação às entidades do tipo referido no anexo I ou II, bem como às entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557;

c) Regras e obrigações em matéria de partilha de informações sobre cibersegurança;

d) Obrigações em matéria de supervisão e execução para os Estados-Membros.

Artigo 2.º

Âmbito de aplicação

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

O artigo 3.º, n.º 4, do anexo da referida recomendação não é aplicável para efeitos da presente diretiva.

2. Independentemente da dimensão que tenham, a presente diretiva também se aplica às entidades de um dos tipos referidos no anexo I ou II, em que:

a) Os serviços são prestados por:

   i) fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público,

   ii) prestadores de serviços de confiança,

   iii) registos de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio;

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

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

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

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

f) A entidade é uma entidade da administração pública:

i) do governo central, tal como definida por um Estado-Membro em conformidade com o direito nacional, ou

ii) a nível regional, tal como definida por um Estado-Membro em conformidade com o direito nacional, que, na sequência de uma avaliação baseada no risco, presta serviços cuja perturbação seria suscetível de ter um impacto significativo nas atividades societais ou económicas críticas.

3. Independentemente da dimensão que tenham, a presente diretiva é aplicável às entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557.

4. Independentemente da dimensão que tenham, a presente diretiva é aplicável às entidades prestadoras de serviços de registo de nomes de domínio.

5. Os Estados-Membros podem prever que a presente diretiva se aplique a:

a) Entidades da administração pública a nível local;

b) Instituições de ensino, em especial quando realizam atividades críticas no domínio da investigação.

6. A presente diretiva não prejudica as responsabilidades dos Estados-Membros de salvaguardar a segurança nacional nem os seus poderes para salvaguardar outras funções essenciais do Estado, nomeadamente para garantir a integridade territorial do Estado e manter a ordem pública.

7. A presente diretiva não se aplica às entidades da administração pública que exercem as suas atividades nos domínios da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo a prevenção, investigação, deteção e repressão de infrações penais.

8. Os Estados-Membros podem isentar entidades específicas que exerçam atividades nos domínios da defesa, da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo a prevenção, investigação, deteção e repressão de infrações penais, ou que ofereçam serviços exclusivamente às entidades da administração púbica a que se refere o n.º 7 do presente artigo, de cumprir as obrigações estabelecidas no artigo 21.º ou 23.º no que diz respeito a essas atividades. Em tais casos, as medidas de supervisão e de execução referidas no capítulo VII não se aplicam a essas atividades ou serviços específicos. Caso as entidades exerçam atividades ou prestem serviços exclusivamente do tipo referido no presente número, os Estados-Membros podem decidir também isentar essas entidades das obrigações previstas nos artigos 3.º e 27.º.

9. Os n.os 7 e 8 não se aplicam quando uma entidade atua como prestador de serviços de confiança.

10. A presente diretiva não se aplica às entidades que os Estados-Membros tenham excluído do âmbito de aplicação do Regulamento (UE) 2022/2554 em conformidade com o artigo 2.º, n.º 4, do referido regulamento.

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

12. A presente diretiva é aplicável sem prejuízo do Regulamento (UE) 2016/679, da Diretiva 2002/58/CE, das Diretivas 2011/93/UE ([27]) e 2013/40/UE do Parlamento Europeu e do Conselho ([28]) e da Diretiva (UE) 2022/2557.

13. Sem prejuízo do artigo 346.º do TFUE, as informações classificadas como confidenciais nos termos de regras da União ou de regras nacionais, tais como regras em matéria de sigilo comercial, só podem ser trocadas com a Comissão e com outras autoridades competentes, em conformidade com a 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 em causa.

([27]) 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).

([28]) 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).

14. As entidades, as autoridades competentes, os pontos de contacto únicos e as CSIRT procedem ao tratamento dos dados pessoais na medida do necessário para efeitos da presente diretiva e em conformidade com o Regulamento (UE) 2016/679, em especial com base no artigo 6.º desse regulamento.

O tratamento de dados pessoais nos termos da presente diretiva por fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público deve ser efetuado em conformidade com o direito da União em matéria de proteção de dados e com o direito da União em matéria de privacidade, nomeadamente a Diretiva 2002/58/CE.

Artigo 3.º

Entidades essenciais e importantes

1. Para efeitos da presente diretiva, consideram-se entidades essenciais as seguintes entidades:

a) Entidades de um dos tipos referidos no anexo I que excedam os limiares para as médias empresas previstos no artigo 2.º, n.º 1, do anexo da Recomendação 2003/361/CE;

b) Prestadores de serviços de confiança qualificados e registos de nomes de domínio de topo, bem como prestadores de serviços de DNS, independentemente da sua dimensão;

c) Fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público que sejam considerados médias empresas nos termos do artigo 2.ºdo anexo da Recomendação 2003/361/CE;

d) Entidades da administração pública a que se refere o artigo 2.º, n.º 2, alínea f), subalínea i);

e) Qualquer outra entidade de um dos tipos referidos no anexo I ou II que um Estado-Membro tenha identificado como entidade essencial nos termos do artigo 2.º, n.º 2, alíneas b) a e);

f) Entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557 a que se refere o artigo 2.º, n.º 3, da presente diretiva;

g) Se o Estado-Membro assim o estabelecer, as entidades que o Estado-Membro em causa tenha identificado antes de 16 de janeiro de 2023 como operadores de serviços essenciais nos termos da Diretiva (UE) 2016/1148 ou do direito nacional.

2. Para efeitos da presente diretiva, são consideradas entidades importantes as entidades de um dos tipos referidos no anexo I ou II que não sejam consideradas entidades essenciais nos termos do n.º 1 do presente artigo. Tal inclui as entidades identificadas pelos Estados-Membros como entidades importantes nos termos do artigo 2.º, n.º 2, alíneas b) a e).

3. Até 17 de abril de 2025, os Estados-Membros estabelecem uma lista das entidades essenciais e importantes, bem como das entidades que prestam serviços de registo de nomes de domínio. Os Estados-Membros revêm e, se for caso disso, atualizam essa lista com regularidade e, pelo menos, de dois em dois anos.

4. Para efeitos do estabelecimento da lista a que se refere o n.º 3, os Estados-Membros requerem às entidades referidas nesse número que apresentem às autoridades competentes, pelo menos, as seguintes informações:

a) Nome da entidade;

b) O endereço e os dados de contacto atualizados, incluindo os endereços de correio eletrónico, as gamas de endereços IP e os números de telefone;

c) Se aplicável, o setor e subsetor pertinentes referidos no anexo I ou II; e

d) Se aplicável, uma lista dos Estados-Membros em que prestam serviços abrangidos pelo âmbito de aplicação da presente diretiva.

As entidades a que se refere o n.º 3 devem notificar sem demora quaisquer alterações dos dados fornecidos nos termos do primeiro parágrafo do presente número e, em qualquer caso, no prazo de duas semanas a contar da data da alteração.

A Comissão, com a assistência da Agência da União Europeia para a Cibersegurança (ENISA), fornece, sem demora injustificada, orientações e modelos no que diz respeito às obrigações estabelecidas no presente número.

Os Estados-Membros podem estabelecer mecanismos nacionais que permitam às entidades registarem-se elas próprias.

5. Até 17 de abril de 2025 e, posteriormente, de dois em dois anos, as autoridades competentes notificam:

a) A Comissão e o grupo de cooperação do número das entidades essenciais e importantes que figuram na lista estabelecida nos termos do n.º 3, para cada um dos setores e subsetores referidos no anexo I ou II; e

b) A Comissão de informações pertinentes sobre o número de entidades essenciais e importantes identificadas nos termos do artigo 2.º, n.º 2, alíneas b) a e), o setor e subsetor referidos no anexo I ou II a que pertencem, o tipo de serviço que prestam e a disposição, de entre as previstas no artigo 2.º, n.º 2, alíneas b) a e), nos termos da qual foram identificadas.

6. Até 17 de abril de 2025 e a pedido da Comissão, os Estados-Membros podem notificar a Comissão dos nomes das entidades essenciais e importantes a que se refere o n.º 5, alínea b).

Artigo 4.º

Atos jurídicos setoriais da União

1. Sempre que atos jurídicos setoriais da União exijam que entidades essenciais e importantes adotem medidas de gestão dos riscos de cibersegurança ou notifiquem incidentes significativos, e se tais requisitos forem, na prática, pelo menos equivalentes às obrigações estabelecidas na presente diretiva, não se aplicam a essas entidades as disposições pertinentes da presente diretiva, nomeadamente as disposições em matéria de supervisão e execução estabelecidas no capítulo VII. Caso os atos jurídicos setoriais da União não abranjam todas as entidades de um setor específico abrangidas pelo âmbito de aplicação da presente diretiva, as disposições pertinentes da presente diretiva continuam a aplicar-se às entidades não abrangidas por esses atos jurídicos setoriais da União.

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 sempre que:

a) As medidas de gestão dos riscos de cibersegurança forem, pelo menos, de efeito equivalente às estabelecidas no artigo 21.º, n.ºs 1 e 2; ou

b) O ato jurídico setorial da União preveja o acesso imediato, se for caso disso automático e direto, às notificações de incidentes por parte das CSIRT, das autoridades competentes ou dos pontos de contacto únicos ao abrigo da presente diretiva e se os requisitos aplicáveis à notificação de incidentes significativos forem, pelo menos, equivalentes aos estabelecidos no artigo 23.º, n.ºs 1 a 6, da presente diretiva.

3. A Comissão fornece, até 17 de julho de 2023, orientações que clarifiquem a aplicação dos n.ºs 1 e 2. A Comissão revê periodicamente essas orientações. Na elaboração dessas orientações, a Comissão tem em conta as observações do grupo de cooperação e da ENISA.

Artigo 5.º

Harmonização mínima

A presente diretiva não obsta a que os Estados-Membros adotem ou mantenham disposições que garantam um elevado nível de cibersegurança, desde que tais disposições sejam compatíveis com as obrigações dos Estados-Membros decorrentes do direito da União.

Artigo 6.º

Definições

Para efeitos da presente diretiva, entende-se por:

1) «Sistema de rede e 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; ou

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 dos sistemas de rede e informação», a capacidade dos sistemas de rede e informação para resistir, com um dado nível de confiança, a eventos suscetíveis de pôr em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por esses sistemas de rede e informação, ou acessíveis por intermédio destes;

3) «Cibersegurança», cibersegurança na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2019/881;

4) «Estratégia nacional de cibersegurança», um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos no domínio da cibersegurança e define a governação com vista à sua consecução no Estado-Membro em causa;

5) «Quase incidente», um evento que poderia ter posto em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou de serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes, que, no entanto, foi possível evitar com êxito ou não se materializou;

6) «Incidente», um 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 sistemas de rede e informação ou acessíveis por intermédio destes;

7) «Incidente de cibersegurança em grande escala», um incidente que cause um nível de perturbação superior à capacidade de resposta de um Estado-Membro ou que tenha um impacto significativo em, pelo menos, dois Estados-Membros;

8) «Tratamento de incidentes», todas as ações e procedimentos que visam a prevenção, a deteção, a análise, a contenção ou a resposta a um incidente e a recuperação de um incidente;

9) «Risco», a possível perda ou perturbação causada por um incidente, expressa como uma combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente;

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

11) «Ciberameaça significativa», uma ciberameaça que, com base nas suas características técnicas, possa ser considerada suscetível de ter um impacto grave nos sistemas de rede e informação de uma entidade ou dos utilizadores dos serviços das entidades, causando danos materiais ou imateriais consideráveis;

12) «Produto de TIC», um produto de TIC na aceção do artigo 2.º, ponto 12, do Regulamento (UE) 2019/881;

13) «Serviço de TIC», um serviço de TIC na aceção do artigo 2.º, ponto 13, do Regulamento (UE) 2019/881;

14) «Processo de TIC», um processo de TIC na aceção do artigo 2.º, ponto 14, do Regulamento (UE) 2019/881;

15) «Vulnerabilidade», um ponto fraco, uma suscetibilidade ou uma falha de um produto de TIC ou de um serviço de TIC passível de ser explorada por uma ciberameaça;

16) «Norma», uma norma na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([29]);

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

([29]) 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).

18) «Ponto de troca de tráfego», 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;

19) «Sistema de nomes de domínio» ou «DNS», um sistema de nomes distribuídos hierarquicamente que possibilita a identificação de serviços e recursos na Internet, permitindo que os dispositivos dos utilizadores finais utilizem os serviços de encaminhamento e de conectividade da Internet para aceder a esses serviços e recursos;

20) «Prestador de serviços de DNS», uma entidade que presta:

a) Serviços de resolução recursiva de nomes de domínio acessíveis ao público para os utilizadores finais de Internet; ou

b) Serviços de resolução com autoridade para nomes de domínio para utilização por terceiros, com exceção dos servidores de nomes raiz;

21) «Registo de nomes de domínio de topo» ou «Registo de nomes de TLD», uma entidade a quem foi delegado um TLD específico e que é responsável pela sua administração, incluindo o registo de nomes de domínio sob o TLD e a operação técnica desse TLD, incluindo a operação dos seus servidores de nomes, a manutenção das suas bases de dados e a distribuição de ficheiros da zona de TLD pelos servidores de nomes, independentemente de qualquer uma destas operações ser executada pela própria entidade ou ser externalizada, mas excluindo situações em que os nomes do TLD sejam utilizados por um registo apenas para uso próprio;

22) «Entidade que presta serviços de registo de nomes de domínio», um agente de registo ou um agente que atua em nome de agentes de registo, tal como um prestador ou revendedor de serviços de proteção da privacidade ou de registo de servidores intermediários;

23) «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 ([30]);

24) «Serviço de confiança», um serviço de confiança na aceção do artigo 3.º, ponto 16, do Regulamento (UE) n.º 910/2014;

25) «Prestador de serviços de confiança», um prestador de serviços de confiança na aceção do artigo 3.º, ponto 19, do Regulamento (UE) n.º 910/2014;

26) «Serviço de confiança qualificado», um serviço de confiança qualificado na aceção do artigo 3.º, ponto 17, do Regulamento (UE) n.º 910/2014;

27) «Prestador qualificado de serviços de confiança», um prestador qualificado de serviços de confiança na aceção do artigo 3.º, ponto 20, do Regulamento (UE) n.º 910/2014;

28) «Mercado em linha», um mercado em linha na aceção do artigo 2.º, alínea n), da Diretiva 2005/29/CE do Parlamento Europeu e do Conselho ([31]);

29) «Motor de pesquisa em linha», um motor de pesquisa em linha na aceção do artigo 2.º, ponto 5, do Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho ([32]);

30) «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;

([30]) 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).

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

([32]) 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).

31) «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 TI que preste serviços de armazenamento, tratamento e transmissão de dados, juntamente com todas as instalações e infraestruturas de distribuição de energia e controlo ambiental;

32) «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;

33) «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;

34) «Representante», qualquer pessoa singular ou coletiva, estabelecida na União, expressamente designada para atuar por conta de um prestador de serviços de DNS, um registo de nomes de TLD, uma entidade que presta serviços de registo de nomes de domínio, um prestador de serviços de computação em nuvem, um prestador de serviços de centro de dados, um fornecedor de redes de distribuição de conteúdos, um prestador de serviços geridos, um prestador de serviços de segurança geridos, um prestador de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais que não se encontre estabelecido 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;

35) «Entidade da administração pública», uma entidade, reconhecida como tal num Estado-Membro, nos termos do direito nacional, não incluindo o poder judicial, os parlamentos ou os bancos centrais, que cumpra os seguintes critérios:

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

   b) É dotada de personalidade jurídica 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, 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;

36) «Rede pública de comunicações eletrónicas», uma rede pública de comunicações eletrónicas na aceção do artigo 2.º, ponto 8, da Diretiva (UE) 2018/1972;

37) «Serviço de comunicações eletrónicas», um serviço de comunicações eletrónicas na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972;

38) «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;

39) «Prestador de serviços geridos», uma entidade que presta serviços relacionados com a instalação, gestão, operação ou manutenção de produtos de TIC, redes, infraestruturas, aplicações ou quaisquer outros sistemas de rede e informação, através de assistência ou administração ativa efetuadas nas instalações dos clientes ou à distância;

40) «Prestador de serviços de segurança geridos», um prestador de serviços geridos que realiza ou presta assistência a atividades relacionadas com a gestão dos riscos de cibersegurança;

41) «Organismo de investigação», uma entidade cujo objetivo principal é realizar investigação aplicada ou desenvolvimento experimental com vista à exploração dos resultados dessa investigação para fins comerciais, excluindo os estabelecimentos de ensino.

CAPÍTULO II

QUADROS COORDENADOS EM MATÉRIA DE CIBERSEGURANÇA

Artigo 7.º

Estratégia nacional de cibersegurança

1. Cada Estado-Membro adota uma estratégia nacional de cibersegurança que estabeleça os objetivos estratégicos, os recursos necessários para atingir esses objetivos e as medidas políticas e regulamentares adequadas, com vista a alcançar e a manter um elevado nível de cibersegurança. A estratégia nacional de cibersegurança inclui:

a) Os objetivos e prioridades da estratégia de cibersegurança do Estado-Membro, abrangendo, em especial, os setores referidos nos anexos I e II;

b) Um quadro de governação para cumprir os objetivos e prioridades referidos na alínea a) do presente número, incluindo as políticas referidas no n.º 2;

c) Um quadro de governação que clarifique as funções e responsabilidades das partes interessadas pertinentes a nível nacional, que consolide a cooperação e coordenação a nível nacional entre as autoridades competentes, os pontos de contacto únicos e as CSIRT ao abrigo da presente diretiva, bem como a coordenação e cooperação entre esses organismos e as autoridades competentes ao abrigo de atos jurídicos setoriais da União;

d) Um mecanismo para identificar ativos pertinentes e uma avaliação dos riscos nesse Estado-Membro;

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

f) Uma lista das diversas autoridades e partes interessadas envolvidas na execução da estratégia nacional de cibersegurança;

g) Um quadro político para o reforço da cooperação entre as autoridades competentes nos termos da presente diretiva e as autoridades competentes nos termos da Diretiva (UE) 2022/2557 para efeitos de partilha de informações sobre riscos, ciberameaças, e incidentes, bem como riscos, ameaças e incidentes não cibernéticos, e do exercício de funções de supervisão, conforme adequado;

h) Um plano, incluindo as medidas necessárias, para reforçar o nível geral de sensibilização dos cidadãos para a cibersegurança.

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

a) Sobre a cibersegurança na cadeia de abastecimento de produtos de TIC e serviços de TIC utilizados pelas entidades na prestação dos seus serviços;

b) Sobre a inclusão e a especificação de requisitos em matéria de cibersegurança aplicáveis a produtos de TIC e serviços de TIC nos procedimentos de contratação pública, incluindo no que respeita à certificação de cibersegurança, à cifragem e à utilização de produtos de cibersegurança de fonte aberta;

c) Que assegurem a gestão das vulnerabilidades, incluindo a promoção e a facilitação da divulgação coordenada de vulnerabilidades nos termos do artigo 12.º, n.º 1;

d) Sobre a manutenção da disponibilidade geral, da integridade e da confidencialidade do núcleo público da Internet aberta, incluindo, quando pertinente, a cibersegurança dos cabos submarinos de comunicações;

e) Que promovam o desenvolvimento e a integração de tecnologias avançadas relevantes que visem a aplicação de medidas de vanguarda em matéria de gestão dos riscos de cibersegurança;

f) Que promovam e desenvolvam a educação e a formação em cibersegurança, as competências no domínio da cibersegurança, a sensibilização e as iniciativas de investigação e desenvolvimento no domínio da cibersegurança, bem como orientações sobre boas práticas e controlos em matéria de ciber-higiene, destinadas aos cidadãos, às partes interessadas e às entidades;

g) Que apoiem as instituições académicas e de investigação no desenvolvimento, na melhoria e na promoção da implantação de ferramentas de cibersegurança e de infraestruturas de redes seguras;

h) Que incluam procedimentos relevantes e ferramentas adequadas de partilha de informações para apoiar a partilha voluntária de informações sobre cibersegurança entre as entidades, em conformidade com o direito da União;

i) Que reforcem a ciber-resiliência e a base de referência em matéria de ciber-higiene das pequenas e médias empresas, especialmente das que estão excluídas do âmbito da presente diretiva, através da disponibilização de orientações e assistência facilmente acessíveis e adaptados às suas necessidades específicas;

j) Que promovam a ciberproteção ativa.

3. Os Estados-Membros devem notificar as suas estratégias nacionais de cibersegurança à Comissão no prazo de três meses a contar da sua adoção. Os Estados-Membros podem excluir informações relacionadas com a sua segurança nacional dessas notificações.

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 atualizá-las. A pedido dos Estados-Membros, a ENISA deve ajudá-los a formular ou a atualizar a estratégia nacional de cibersegurança e indicadores-chave de desempenho para a avaliação dessa estratégia, a fim de a alinhar com os requisitos e obrigações estabelecidos na presente diretiva.

Artigo 8.º

Autoridades competentes e pontos de contacto únicos

1. Cada Estado-Membro deve designar ou criar uma ou várias autoridades competentes responsáveis pela cibersegurança e pelo desempenho das funções de supervisão estabelecidas no capítulo VII (autoridades competentes).

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 ou criar um ponto de contacto único. Caso um Estado-Membro designe ou crie apenas uma autoridade competente nos termos do n.º 1, 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, se for caso disso, com a Comissão e a ENISA, bem como para assegurar a cooperação transetorial com outras autoridades competentes do seu Estado-Membro.

5. Os Estados-Membros devem certificar-se de que as suas autoridades competentes e 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.

6. Cada Estado-Membro deve notificar a Comissão, sem demora injustificada, da identidade 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 respetivas funções e de quaisquer alterações posteriores das mesmas. Cada Estado-Membro deve publicar a identidade da sua autoridade competente. A Comissão deve publicar uma lista dos pontos de contacto únicos.

Artigo 9.º

Quadros nacionais de gestão de cibercrises

1. Os Estados-Membros devem designar ou criar uma ou várias autoridades competentes responsáveis pela gestão de crises e de incidentes de cibersegurança em grande escala (autoridades de gestão de cibercrises). Os Estados-Membros devem assegurar que essas autoridades 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 a nível nacional.

2. Caso um Estado-Membro designe ou crie mais do que uma autoridade de gestão de cibercrises referida no n.º 1, deve indicar claramente qual dessas autoridades assume o papel de coordenadora para a gestão de crises e de incidentes de cibersegurança em grande escala.

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

4. Cada Estado-Membro deve adotar um plano nacional de resposta a crises e a incidentes de cibersegurança em grande escala que estabeleça os objetivos e as modalidades de gestão de crises e de incidentes de cibersegurança em grande escala. Esse plano deve estabelecer, nomeadamente:

a) Os objetivos das atividades e medidas nacionais de preparação;

b) As funções e responsabilidades das autoridades de gestão de cibercrises;

c) Os procedimentos de gestão de cibercrises, incluindo a sua integração no quadro geral de gestão de crises e canais de intercâmbio de informações;

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

e) As partes interessadas pertinentes dos setores público e privado e infraestruturas envolvidas;

f) Os 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.

5. No prazo de três meses a contar da designação ou criação da autoridade de gestão de cibercrises a que se refere o n.º 1, cada Estado-Membro deve notificar a Comissão da identidade da sua autoridade e de quaisquer alterações subsequentes da mesma. Os Estados-Membros devem apresentar à Comissão e à Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) informações pertinentes sobre os requisitos do n.º 4 sobre os respetivos planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala no prazo de três meses a contar da adoção desses planos. Os Estados-Membros podem excluir informações, na medida em que essa exclusão seja necessária para salvaguardar a sua segurança nacional.

Artigo 10.º

Equipas de resposta a incidentes de segurança informática (CSIRT)

1. Cada Estado-Membro deve designar ou criar uma ou várias CSIRT. As CSIRT podem ser designadas ou criadas no seio de uma autoridade competente. As CSIRT devem cumprir os requisitos estabelecidos no artigo 11.º, n.º 1, devem abranger pelo menos os setores, subsetores e tipos de entidades referidos nos anexos I e II, e devem ser responsáveis pelo tratamento de incidentes de acordo com um processo bem definido.

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 11.º, n.º 3.

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

4. As CSIRT devem cooperar e, se for caso disso, trocar informações importantes, em conformidade com o artigo 29.º, com comunidades setoriais ou transetoriais de entidades essenciais e importantes.

5. As CSIRT devem participar em avaliações pelos pares organizadas nos termos do artigo 19.º.

6. Os Estados-Membros devem garantir a cooperação eficaz, eficiente e segura das suas CSIRT no âmbito da rede de CSIRT.

7. As CSIRT podem estabelecer relações de cooperação com equipas nacionais de resposta a incidentes de segurança informática de países terceiros. No âmbito dessas relações de cooperação, os Estados-Membros devem facilitar um intercâmbio de informações eficaz, eficiente e seguro com as referidas equipas nacionais de resposta a incidentes de segurança informática de países terceiros, utilizando protocolos pertinentes de partilha de informações, nomeadamente o protocolo «sinalização luminosa». As CSIRT podem trocar informações pertinentes com equipas nacionais de resposta a incidentes de segurança informática de países terceiros, incluindo dados pessoais, em conformidade com o direito da União em matéria de proteção de dados.

8. As CSIRT podem cooperar com equipas nacionais de resposta a incidentes de segurança informática de países terceiros ou organismos equivalentes de países terceiros, nomeadamente para lhes prestar assistência em matéria de cibersegurança.

9. Cada Estado-Membro deve notificar a Comissão, sem demora injustificada, da identidade da CSIRT a que se refere o n.º 1 do presente artigo e da CSIRT coordenadora designada nos termos do artigo 12.º, n.º 1, das respetivas funções em relação a entidades essenciais e importantes e de quaisquer alterações posteriores das mesmas.

10. Os Estados-Membros podem solicitar a assistência da ENISA na criação das respetivas CSIRT.

Artigo 11.º

Requisitos, capacidades técnicas 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 assegurar a confidencialidade e a credibilidade das suas operações;

e) As CSIRT devem dispor de pessoal suficiente para assegurar a disponibilidade dos seus serviços em qualquer momento e devem garantir que o seu pessoal tem formação adequada;

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

As CSIRT podem participar em redes de cooperação internacional.

2. Os Estados-Membros devem assegurar que as respetivas CSIRT dispõe conjuntamente das capacidades técnicas necessárias para desempenhar as funções referidas no n.º 3. Os Estados-Membros devem assegurar a afetação de recursos suficientes às suas CSIRT, a fim de assegurar níveis de pessoal adequados para efeitos de permitir às CSIRT desenvolver as suas capacidades técnicas.

3. As funções das CSIRT são as seguintes:

a) Monitorizar e analisar ciberameaças, vulnerabilidades e incidentes a nível nacional e, mediante pedido, prestar assistência a entidades essenciais e importantes em causa relativamente à monitorização em tempo real ou quase real dos seus sistemas de rede e informação;

b) Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às entidades essenciais e importantes, bem como a autoridades competentes e a outras partes interessadas, sobre ciberameaças, vulnerabilidades e incidentes, se possível em tempo quase real;

c) Intervir em caso de incidentes e prestar assistência às entidades essenciais e importantes envolvidas, se aplicável;

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, a pedido de uma entidade essencial ou importante, uma análise proativa dos sistemas de rede e informação da entidade em causa, a fim de detetar vulnerabilidades com um potencial impacto significativo;

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

g) Se aplicável, atuar como coordenador para efeitos do processo de divulgação coordenada de vulnerabilidades a que se refere o artigo 12.º, n.º 1;

h) Contribuir para a implantação de ferramentas seguras de partilha de informações nos termos do artigo 10.º, n.º 3.

As CSIRT podem realizar uma análise proativa e não intrusiva de sistemas de rede e informação acessíveis ao público de entidades essenciais e importantes. Essa análise deve ser efetuada com o objetivo de detetar sistemas de rede e informação vulneráveis ou inseguros e de informar as entidades em causa. Essa análise não deve ter qualquer impacto negativo no funcionamento dos serviços das entidades.

No exercício das funções a que se refere o primeiro parágrafo, as CSIRT podem dar prioridade a determinadas tarefas com base numa abordagem baseada no risco.

4. As CSIRT devem estabelecer relações de cooperação com as partes interessadas pertinentes do setor privado, com vista a alcançar da melhor forma os objetivos da presente diretiva.

5. A fim de facilitar a cooperação referida no n.º 4, 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; e

c) Divulgação coordenada de vulnerabilidades nos termos do artigo 12.º, n.º 1.

Artigo 12.º

Divulgação coordenada de vulnerabilidades e base de dados europeia de vulnerabilidades

1. Cada Estado-Membro deve designar uma das suas CSIRT como coordenadora para efeitos da divulgação coordenada de vulnerabilidades. A CSIRT designada coordenadora deve desempenhar o papel de intermediário de confiança, facilitando, quando necessário, a interação entre a pessoa singular ou coletiva notificadora e o fabricante ou fornecedor de produtos de TIC ou prestador de serviços de TIC que sejam potencialmente vulneráveis, a pedido de qualquer uma das partes. As funções da CSIRT designada coordenadora devem incluir:

a) A identificação e o contacto das entidades em causa;

b) A prestação de apoio às pessoas singulares ou coletivas que notifiquem as vulnerabilidades; e

c) A negociação do calendário de divulgação e a gestão das vulnerabilidades que afetem várias entidades.

Os Estados-Membros devem assegurar que as pessoas singulares ou coletivas possam comunicar uma vulnerabilidade à CSIRT designada coordenadora, de forma anónima se assim o solicitarem. A CSIRT designada coordenadora assegura a realização de ações de acompanhamento diligentes no que diz respeito à vulnerabilidade comunicada e assegura o anonimato da pessoa singular ou coletiva que comunica a vulnerabilidade. Nos casos em que a vulnerabilidade notificada possa ter um impacto importante sobre entidades em mais do que um Estado-Membro, a CSIRT designada como coordenadora por cada Estado-Membro em causa deve, se for caso disso, cooperar com outras CSIRT designadas como coordenadoras no âmbito da rede de CSIRT.

2. Após consulta do grupo de cooperação, a ENISA deve criar e manter uma base de dados europeia de vulnerabilidades. Para tal, deve estabelecer e manter sistemas de informação, políticas e procedimentos adequados, e adotar as medidas técnicas e organizativas necessárias para assegurar a segurança e a integridade da base de dados europeia de vulnerabilidades, tendo em vista, em especial, permitir que entidades, independentemente de estarem abrangidas pelo âmbito da presente diretiva, e os respetivos fornecedores de sistemas de rede e informação, divulguem e registem, a título voluntário, vulnerabilidades publicamente conhecidas presentes nos produtos de TIC ou serviços de TIC. Todas as partes interessadas devem ter acesso às informações sobre as vulnerabilidades constantes da base de dados europeia de vulnerabilidades. A referida base de dados deve incluir:

a) Informações que descrevam a vulnerabilidade;

b) Os produtos de TIC ou os serviços de TIC afetados e a gravidade da vulnerabilidade em termos das circunstâncias em que pode ser explorada;

c) A disponibilidade de correções e, na falta de correções, orientações fornecidas pelas autoridades competentes ou CSIRT destinadas aos utilizadores de produtos de TIC e serviços de TIC vulneráveis sobre formas de minimizar os riscos resultantes das vulnerabilidades divulgadas.

Artigo 13.º

Cooperação a nível nacional

1. Se forem entidades distintas, as autoridades competentes, o ponto de contacto único e as 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 CSIRT ou, se aplicável, as respetivas autoridades competentes recebem notificações sobre incidentes significativos, nos termos do artigo 23.º, e sobre incidentes, ciberameaças e quase incidentes, nos termos do artigo 30.º.

3. Os Estados-Membros devem assegurar que as respetivas CSIRT ou, se aplicável, as respetivas autoridades competentes informam o seu ponto de contacto único das notificações de incidentes, ciberameaças e quase incidentes efetuadas nos termos da presente diretiva.

4. A fim de assegurar que as funções e obrigações das autoridades competentes, dos pontos de contacto únicos e das CSIRT são desempenhadas de forma eficaz, os Estados-Membros devem assegurar, na medida do possível, uma cooperação adequada entre esses organismos e as autoridades policiais, as autoridades de proteção de dados, as autoridades nacionais nos termos dos Regulamentos (CE) n.º 300/2008 e (UE) 2018/1139, os organismos de supervisão nos termos do Regulamento (UE) n.º 910/2014, as autoridades competentes anos termos do Regulamento (UE) 2022/2554, as autoridades reguladoras nacionais nos termos da Diretiva (UE) 2018/1972, as autoridades competentes nos termos da Diretiva (UE) 2022/2557, bem como as autoridades competentes nos termos de outros atos jurídicos setoriais da União no âmbito desse Estado-Membro.

5. Os Estados-Membros devem assegurar que as respetivas autoridades competentes nos termos da presente diretiva e as respetivas autoridades competentes nos termos da Diretiva (UE) 2022/2557 cooperam e trocam regularmente informações sobre a identificação de entidades críticas, sobre riscos, ciberameaças e incidentes, bem como sobre riscos, ameaças e incidentes não cibernéticos que afetem entidades essenciais identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557, bem como as medidas adotadas em resposta a esses riscos, ameaças e incidentes. Os Estados-Membros devem assegurar igualmente que as respetivas autoridades competentes ao abrigo da presente diretiva e as respetivas autoridades competentes nos termos do Regulamento (UE) n.º 910/2014, do Regulamento (UE) 2022/2554 e da Diretiva (UE) 2018/1972 troquem regularmente informações pertinentes, nomeadamente no que diz respeito a incidentes e ciberameaças relevantes.

6. Os Estados-Membros simplificam a comunicação de informações através de meios técnicos para as notificações a que se referem os artigos 23.º e 30.º.

CAPÍTULO III

COOPERAÇÃO A NÍVEL DA UNIÃO E A NÍVEL INTERNACIONAL

Artigo 14.º

Grupo de cooperação

1. É criado um grupo de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros, 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 7.

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 ao abrigo do Regulamento (UE) 2022/2554 podem participar nas atividades do grupo de cooperação nos termos do artigo 47.º, n.º 1, do referido regulamento.

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

O secretariado do grupo é assegurado pela Comissão.

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

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

b) Fornecer orientações às autoridades competentes sobre a elaboração e a execução de políticas em matéria de divulgação coordenada de vulnerabilidades, tal como se refere no artigo 7.º, n.º 2, alínea c);

c) 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, bem como a identificação de entidades essenciais e importantes nos termos do artigo 2.º, n.º 2, alíneas b) a e);

d) Trocar pareceres e cooperar com a Comissão em novas iniciativas políticas no domínio da cibersegurança e da coerência global dos requisitos de cibersegurança setoriais;

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

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

g) Proceder a trocas de pontos de vista sobre a aplicação de atos jurídicos setoriais da União que contenham disposições em matéria de cibersegurança;

h) Quando pertinente, discutir os relatórios das avaliações pelos pares a que se refere o artigo 19.º, n.º 9, e elaborar conclusões e recomendações;

i) Realizar avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas, em conformidade com o artigo 22.º, n.º 1;

j) Discutir casos de assistência mútua, incluindo experiências e os resultados de ações de supervisão conjunta transfronteiriça a que se refere o artigo 37.º;

k) A pedido de um ou mais Estados-Membros envolvidos, discutir os pedidos específicos de assistência mútua a que se refere o artigo 37.º;

l) Fornecer orientações estratégicas à rede de CSIRT e à UE–CyCLONe sobre questões emergentes específicas;

m) Proceder a trocas de pontos de vista sobre a política em matéria de ações de acompanhamento na sequência de crises e de incidentes de cibersegurança em grande escala, com base nos ensinamentos retirados da rede de CSIRT e da UE-CyCLONe;

n) 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;

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

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

q) Estabelecer a metodologia e os aspetos organizacionais das avaliações pelos pares a que se refere o artigo 19.º, n.º 1, bem como estabelecer a metodologia de autoavaliação para os Estados-Membros nos termos do artigo 19.º, n.º 5, com a assistência da Comissão e da ENISA, e, em cooperação com a Comissão e a ENISA, elaborar códigos de conduta subjacentes aos métodos de trabalho dos peritos em cibersegurança designados nos termos do artigo 19.º, n.º 6;

r) Para efeitos da avaliação a que se refere o artigo 40.º, preparar relatórios sobre a experiência adquirida a nível estratégico e através de avaliações pelos pares;

s) Discutir e realizar regularmente uma avaliação do ponto da situação das ciberameaças ou incidentes, como o *ransomware*.

O grupo de cooperação apresenta os relatórios referidos no primeiro parágrafo, alínea r), à Comissão, ao Parlamento Europeu e ao Conselho.

5. Os Estados-Membros garantem a cooperação eficaz, eficiente e segura dos respetivos representantes no grupo de cooperação.

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

7. Até 1 de fevereiro de 2024 e, posteriormente, 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.

8. 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 39.º, n.º 2.

A Comissão deve proceder ao intercâmbio de aconselhamentos e cooperar com o grupo de cooperação sobre os projetos de atos de execução referidos no primeiro parágrafo do presente número, em conformidade com o n.º 4, alínea e).

9. O grupo de cooperação reúne-se regularmente, e, em qualquer caso, pelo menos uma vez por ano, com o grupo para a resiliência das entidades críticas criado nos termos da Diretiva (UE) 2022/2557, com vista a promover e a facilitar a cooperação estratégica e o intercâmbio de informações.

Artigo 15.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 designadas ou criadas nos termos do artigo 10.º e da Equipa de Resposta a Emergências Informáticas para as instituições, organismos e agências da União (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) Facilitar a partilha, a transferência e o intercâmbio de tecnologia e de medidas, políticas, ferramentas, processos, melhores práticas e quadros pertinentes entre as CSIRT;

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

d) Proceder ao intercâmbio de informações sobre publicações e recomendações em matéria de cibersegurança;

e) Assegurar a interoperabilidade no que diz respeito às especificações e protocolos de partilha de informações;

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

g) 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;

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

i) Cooperar, trocar boas práticas e prestar assistência às CSIRT designadas coordenadoras nos termos do artigo 12.º, n.º 1, relativamente à gestão da divulgação coordenada de vulnerabilidades que possam ter um impacto significativo nas entidades de mais do que um Estado-Membro;

j) 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 em grande escala a que se refere o artigo 9.º, n.º 4, a pedido de um Estado-Membro;

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

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

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

n) 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;

o) Quando pertinente, discutir os relatórios das avaliações pelos pares a que se refere o artigo 19.º, n.º 9;

p) Fornecer 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. Até 17 de janeiro de 2025, e, posteriormente, de dois em dois anos, a rede de CSIRT deve avaliar os progressos alcançados no domínio da cooperação operacional e apresentar um relatório, para efeitos da avaliação a que se refere o artigo 40.º. Em especial, o relatório deve expor conclusões e fazer recomendações sobre os resultados das avaliações pelos pares realizadas nos termos do artigo 19.º em relação às CSIRT nacionais. Esse relatório deve ser apresentado ao grupo de cooperação.

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

6. A rede de CSIRT e a UE-CyCLONe devem acordar disposições processuais e cooperar com base nessas disposições.

Artigo 16.º

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

1. É criada a 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 pertinentes 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 cibercrises dos Estados-Membros, bem como, nos casos em que um incidente de cibersegurança em grande escala, potencial ou em curso, tenha ou seja suscetível de ter um impacto significativo nos serviços e atividades abrangidos pelo âmbito de aplicação da presente diretiva, pela Comissão. Noutros casos, a Comissão participa nas atividades da UE-CyCLONe na qualidade de observadora.

A ENISA assegura os serviços de secretariado da UE-CyCLONe e presta apoio ao intercâmbio seguro de informações, bem como 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 crises e de incidentes de cibersegurança em grande escala;

b) Desenvolver um conhecimento situacional comum relativo a crises e incidentes de cibersegurança em grande escala;

c) Avaliar as consequências e o impacto de crises e incidentes de cibersegurança em grande escala relevantes e propor eventuais medidas de atenuação;

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

e) Discutir, a pedido do Estado-Membro em causa, os planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala a que se refere o artigo 9.º, n.º 4.

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

5. A UE-CyCLONe presta informações ao grupo de cooperação sobre a gestão de crises e de incidentes de cibersegurança em grande escala, bem como sobre tendências, dedicando especial atenção ao seu impacto em entidades essenciais e importantes.

6. A UE-CyCLONe coopera com a rede de CSIRT com base nas disposições processuais acordadas previstas no artigo 15.º, n.º 6.

7. Até 17 de julho de 2024, e, subsequentemente, a intervalos de 18 meses, a UE-CyCLONe apresenta ao Parlamento Europeu e ao Conselho um relatório de avaliação do seu trabalho.

Artigo 17.º

Cooperação internacional

Se for caso disso, 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 determinadas atividades do grupo de cooperação, da rede de CSIRT e da UE-CyCLONe. Esses acordos devem respeitar o direito da União em matéria de proteção de dados.

Artigo 18.º

Relatório sobre o estado da cibersegurança na União

1. A ENISA deve adotar, em cooperação com a Comissão e com o grupo de cooperação, um relatório bienal sobre o estado da cibersegurança na União e deve transmitir e apresentar esse relatório ao Parlamento Europeu. Este relatório deve, nomeadamente, ser disponibilizado em formato legível por máquina e incluir:

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

b) Uma avaliação do desenvolvimento das capacidades de cibersegurança nos setores público e privado em toda a União;

c) Uma avaliação do nível geral de sensibilização para a cibersegurança e a ciber-higiene entre os cidadãos e as entidades, incluindo as pequenas e médias empresas;

d) Uma avaliação agregada dos resultados das avaliações pelos pares a que se refere o artigo 19.º;

e) Uma avaliação agregada do nível de maturidade das capacidades e dos recursos em matéria de cibersegurança em toda a União, incluindo a nível setorial, bem como do grau de alinhamento das estratégias nacionais de cibersegurança dos Estados-Membros.

2. O relatório deve incluir recomendações políticas específicas, com vista a colmatar lacunas e 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 no que se refere a incidentes e ciberameaças elaborados pela ENISA em conformidade com o artigo 7.º, n.º 6, do Regulamento (UE) 2019/881.

3. A ENISA, em cooperação com a Comissão, o grupo de cooperação e a rede de CSIRT, deve elaborar a metodologia, incluindo as variáveis pertinentes, como os indicadores quantitativos e qualitativos, da avaliação agregada a que se refere o n.º 1, alínea e).

Artigo 19.º

Avaliações pelos pares

1. O mais tardar a 17 de janeiro de 2025, o grupo de cooperação estabelece, com a assistência da Comissão e da ENISA e, quando pertinente, da rede de CSIRT, a metodologia e os aspetos organizacionais das avaliações pelos pares, com vista a retirar ensinamentos das experiências partilhadas, reforçar a confiança mútua, alcançar um elevado nível comum de cibersegurança e reforçar as capacidades e políticas de cibersegurança dos Estados-Membros necessárias à aplicação da presente diretiva. A participação nas avaliações pelos pares é voluntária. As avaliações pelos pares devem ser realizadas por peritos em cibersegurança. Os peritos em cibersegurança são designados por, pelo menos, dois Estados-Membros, diferentes do Estado-Membro avaliado.

As avaliações pelos pares devem incidir, no mínimo, num dos seguintes aspetos:

a) O nível de aplicação das medidas de gestão dos riscos de cibersegurança e das obrigações de notificação previstos nos artigos 21.º e 23.º;

b) O nível de capacidades, incluindo os recursos financeiros, técnicos e humanos disponíveis, e a eficácia das autoridades competentes no desempenho das suas funções;

c) As capacidades operacionais das CSIRT;

d) O nível de aplicação da assistência mútua a que se refere o artigo 37.º;

e) O nível de aplicação dos acordos de partilha de informações em matéria de cibersegurança a que se refere o artigo 29.º;

f) Questões específicas de natureza transfronteiriça ou intersetorial.

2. A metodologia referida no n.º 1 deve incluir critérios objetivos, não discriminatórios, equitativos e transparentes com base nos quais os Estados-Membros designam os peritos em cibersegurança elegíveis para realizarem as avaliações pelos pares. A Comissão e a ENISA participam nas avaliações pelos pares na qualidade de observadores.

3. Os Estados-Membros podem identificar questões específicas referidas no n.º 1, alínea f), para efeitos de avaliação pelos pares.

4. Antes de iniciar uma avaliação pelos pares como referido no n.º 1, os Estados Membros notificam os Estados-Membros participantes do âmbito da referida avaliação, incluindo as questões específicas identificadas nos termos do n.º 3.

5. Antes do início da avaliação pelos pares, os Estados-Membros podem efetuar uma autoavaliação dos aspetos analisados e facultar essa autoavaliação aos peritos em cibersegurança designados. O grupo de cooperação estabelece, com a assistência da Comissão e da ENISA, a metodologia para a autoavaliação pelos Estados-Membros.

6. As avaliações pelos pares devem incluir visitas virtuais ou físicas aos locais e intercâmbios de informação fora do local. Tendo em conta o princípio da boa cooperação, os Estados-Membros que sejam objeto da avaliação pelos pares devem facultar aos peritos em cibersegurança designados as informações que sejam necessárias para a avaliação, sem prejuízo do direito da União ou nacional relacionado com a proteção de informações confidenciais ou classificadas e com a salvaguarda de funções essenciais do Estado, tais como a segurança nacional. O grupo de cooperação, em cooperação com a Comissão e a ENISA, deve elaborar códigos de conduta adequados nos quais devem assentar os métodos de trabalho dos peritos em cibersegurança designados. As informações obtidas durante a avaliação pelos pares devem ser utilizadas exclusivamente para esse fim. Os peritos em cibersegurança que participam na avaliação pelos pares não podem divulgar a terceiros quaisquer informações sensíveis ou confidenciais obtidas no decurso da referida avaliação.

7. Os aspetos que tenham sido objeto de uma avaliação pelos pares num Estado-Membro não serão objeto de uma nova avaliação pelos pares nesse Estado-Membro nos dois anos seguintes à conclusão da avaliação pelos pares, salvo em caso de pedido em contrário do Estado-Membro ou de decisão nesse sentido na sequência de uma proposta do grupo de cooperação.

8. Os Estados-Membros devem assegurar que qualquer risco de conflito de interesses respeitante aos peritos em cibersegurança designados é revelado, antes do início da avaliação pelos pares, aos outros Estados-Membros, ao grupo de cooperação, à Comissão e à ENISA. O Estado-Membro que é objeto de uma avaliação pelos pares pode opor-se à designação de determinados peritos em cibersegurança por motivos devidamente fundamentados comunicados ao Estado-Membro que os designa.

9. Os peritos em cibersegurança que participam nas avaliações pelos pares devem elaborar relatórios sobre as constatações e conclusões dessas avaliações pelos pares. Os Estados-Membros que são objeto de avaliação pelos pares podem apresentar observações sobre os projetos de relatório que lhes digam respeito, devendo essas observações ser anexadas aos relatórios. Os relatórios devem incluir recomendações que permitam melhorar os aspetos abrangidos pela avaliação pelos pares. Os relatórios devem ser apresentados ao grupo de cooperação e à rede de CSIRT, quando pertinente. Um Estado-Membro objeto de avaliação pelos pares pode decidir tornar público o seu relatório ou uma versão expurgada do mesmo.

CAPÍTULO IV

MEDIDAS DE GESTÃO DOS RISCOS DE CIBERSEGURANÇA E OBRIGAÇÕES DE NOTIFICAÇÃO

Artigo 20.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 21.º, supervisionam a sua aplicação e podem ser responsabilizados por infrações cometidas pelas entidades referidas nesse artigo.

O presente número aplica-se sem prejuízo do direito nacional no que respeita às regras em matéria de responsabilidade aplicáveis às instituições públicas, bem como à responsabilidade dos funcionários públicos e dos funcionários eleitos ou nomeados.

2. Compete igualmente aos Estados-Membros garantir que os membros do órgão de direção das entidades essenciais e importantes sejam obrigados a frequentar ações de formação e incentivar as entidades essenciais e importantes a oferecer regularmente ações de formação semelhantes aos seus trabalhadores, a fim de adquirirem conhecimentos e competências suficientes para identificarem e avaliarem as práticas de gestão dos riscos de cibersegurança, bem como o seu impacto nos serviços prestados pela entidade.

Artigo 21.º

Medidas de gestão dos riscos de cibersegurança

1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes tomam medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança dos sistemas de rede e informação que utilizam nas suas operações ou na prestação dos seus serviços e para impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços.

As medidas referidas no primeiro parágrafo devem garantir um nível de segurança dos sistemas de rede e informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes e, se aplicáveis, as normas europeias e internacionais pertinentes, bem como os custos de execução. Ao avaliar a proporcionalidade dessas medidas, deve ser tido em devida conta o grau de exposição da entidade aos riscos, a dimensão da entidade e a probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

2. As medidas referidas no n.º 1 devem basear-se numa abordagem que abranja todos os riscos e que vise proteger os sistemas de rede e informação, bem como o seu ambiente físico contra incidentes, e devem abranger pelo menos os seguintes aspetos:

a) Políticas de análise dos riscos e de segurança dos sistemas de informação;

b) Tratamento de incidentes;

c) Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises;

d) Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos;

e) Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e 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) Práticas básicas de ciber-higiene e formação em cibersegurança;

h) Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem;

i) Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos;

j) Utilização de soluções de autenticação multifatores ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, se for caso disso.

3. Os Estados-Membros devem garantir que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), do presente artigo, as entidades têm 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 avaliarem quais das medidas a que se refere essa alínea, são adequadas, as entidades são obrigadas a ter em conta os resultados das avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas realizadas nos termos do artigo 22.º, n.º 1.

4. Os Estados-Membros devem assegurar que uma entidade que conclua que não cumpre as medidas estabelecidas no n.º 2 tome todas as medidas corretivas necessárias, adequadas e proporcionadas, sem demora injustificada.

5. Até 17 de outubro de 2024, a Comissão deve adotar atos de execução que estabeleçam os requisitos técnicos e metodológicos das medidas referidas no n.º 2 no que respeita aos prestadores de serviços de DNS, aos registos de nomes de TLD, aos prestadores de serviços de computação em nuvem, aos prestadores de serviços de centro de dados, aos fornecedores de redes de distribuição de conteúdos, aos prestadores de serviços geridos, aos prestadores de serviços de segurança geridos, bem como aos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais e aos prestadores de serviços de confiança.

A Comissão pode adotar atos de execução que estabeleçam os requisitos técnicos e metodológicos, bem como os requisitos setoriais, se necessário, das medidas a que se refere o n.º 2 no que diz respeito às entidades essenciais e importantes que não as referidas no primeiro parágrafo do presente número.

Na preparação dos atos de execução referidos no primeiro e no segundo parágrafos do presente número, a Comissão segue, tanto quanto possível, as normas europeias e internacionais, bem como as especificações técnicas aplicáveis. A Comissão deve proceder ao intercâmbio de aconselhamentos e cooperar com o grupo de cooperação e com a ENISA sobre os projetos de atos de execução, em conformidade com o artigo 14.º, n.º 4, alínea e).

Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 22.º

Avaliações coordenadas a nível da União dos riscos de segurança de cadeias de abastecimento 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 abastecimento de produtos de TIC, sistemas de TIC 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 e, se necessário, das partes interessadas pertinentes, a Comissão deve identificar os produtos de TIC, sistemas de TIC ou serviços de TIC críticos específicos que podem ser sujeitos à avaliação coordenada dos riscos de segurança a que se refere o n.º 1.

Artigo 23.º

Obrigações de notificação

1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam a sua CSIRT ou, se aplicável, a sua autoridade competente, sem demora injustificada e nos termos do n.º 4, de qualquer incidente que tenha um impacto significativo na prestação dos seus serviços, tal como referido no n.º 3 (incidente significativo). Se for caso disso, as entidades em causa devem notificar os destinatários dos seus serviços, sem demora injustificada, de incidentes significativos suscetíveis de afetar negativamente a prestação desses serviços. Compete a cada Estado-Membro garantir que as referidas entidades comunicam, nomeadamente, quaisquer informações que permitam à CSIRT ou, se aplicável, à autoridade competente determinar o eventual impacto transfronteiriço do incidente. A mera notificação não sujeita a entidade notificadora a responsabilidades acrescidas.

Sempre que as entidades em causa notifiquem a autoridade competente de um incidente significativo nos termos do primeiro parágrafo, o Estado-Membro vela por que essa autoridade competente transmita a notificação à CSIRT após a sua receção.

Em caso de incidente transfronteiriço ou intersetorial significativo, os Estados-Membros devem assegurar que os seus pontos de contacto únicos recebam em tempo útil as informações pertinentes notificadas em conformidade com o n.º 4.

2. Quando aplicável, os Estados-Membros devem assegurar que as entidades essenciais e importantes comuniquem, sem demora injustificada, aos destinatários dos seus serviços potencialmente afetados por uma ciberameaça significativa as medidas ou soluções que estes podem adotar para responder a essa ameaça. Se for caso disso, as entidades devem igualmente informar os referidos destinatários da própria ciberameaça significativa.

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

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

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

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

a) Sem demora injustificada e, em qualquer caso, no prazo de 24 horas depois de terem tomado conhecimento do incidente significativo, um alerta rápido, que, se aplicável, deve indicar se há suspeitas de que o incidente significativo foi causado por um ato ilícito ou malicioso ou se pode ter um impacto transfronteiriço;

b) Sem demora injustificada e, em qualquer caso, no prazo de 72 horas depois de terem tomado conhecimento do incidente significativo, uma notificação de incidente, que, se aplicável, deve atualizar as informações a que se refere a alínea a) e fornecer uma avaliação inicial do incidente significativo, incluindo da sua gravidade e do seu impacto, bem como, se disponíveis, dos indicadores de exposição a riscos;

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

d) O mais tardar um mês após a apresentação da notificação de incidente mencionada na alínea b), um relatório final que contenha os seguintes elementos:

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

   ii) o tipo de ameaça ou provável causa primária suscetível de ter desencadeado o incidente,

   iii) medidas de atenuação aplicadas e em curso,

   iv) se aplicável, o impacto transfronteiriço do incidente;

e) Em caso de incidente em curso no momento da apresentação do relatório final referido na alínea d), os Estados-Membros devem assegurar que as entidades em causa apresentem um relatório intercalar nessa altura e um relatório final no prazo de um mês após terem resolvido o incidente.

Em derrogação do disposto no primeiro parágrafo, alínea b), um prestador de serviços de confiança notifica a CSIRT ou, se aplicável, a autoridade competente, sem demora injustificada e, em qualquer caso, no prazo de 24 horas após ter tomado conhecimento do incidente significativo, de qualquer incidente significativo que afete a prestação dos seus serviços de confiança.

5. Sem demora injustificada e, se possível, no prazo de 24 horas após a receção do alerta rápido a que se refere o n.º 4, alínea a), a CSIRT ou a autoridade competente devem apresentar uma resposta à entidade notificadora que forneça, designadamente, as suas observações iniciais sobre o incidente significativo e, a pedido da entidade, orientações ou aconselhamento operacional sobre a aplicação de possíveis medidas de atenuação. Nos casos em que a CSIRT não seja o destinatário inicial da notificação a que se refere o n.º 1, as orientações devem ser fornecidas pela autoridade competente, em cooperação 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 significativo, o CSIRT ou a autoridade competente devem fornecer igualmente orientações sobre a notificação do incidente significativo às autoridades policiais.

6. Se for caso disso, e em particular se o incidente significativo a que se refere o n.º 1 disser respeito a dois ou mais Estados-Membros, a CSIRT, a autoridade competente ou o ponto de contacto único devem informar, sem demora injustificada, os outros Estados-Membros afetados e a ENISA do incidente significativo. Essas informações devem incluir o tipo de informações recebidas em conformidade com o n.º 4. Ao fazê-lo, a CSIRT, a autoridade competente ou o ponto de contacto único devem salvaguardar, de acordo com o direito da União ou nacional, 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 significativo ou para responder a um incidente significativo em curso, ou em que a divulgação do incidente significativo seja de interesse público, a CSIRT de um Estado-Membro ou, se aplicável, a sua autoridade competente e, se for caso disso, as CSIRT ou as autoridades competentes dos outros Estados-Membros afetados podem, após consulta da entidade em causa, informar o público do incidente significativo ou exigir que a entidade o faça.

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

9. O ponto de contacto único deve apresentar à ENISA, a intervalos de três meses, um relatório de síntese que inclua dados anonimizados e agregados sobre os incidentes significativos, os incidentes, as ciberameaças e os quase incidentes notificados nos termos do n.º 1 do presente artigo e do artigo 30.º A fim de contribuir para a comparabilidade das informações apresentadas, a ENISA pode adotar orientações técnicas sobre os parâmetros das informações a incluir no relatório de síntese. A ENISA deve informar o grupo de cooperação e a rede de CSIRT das suas conclusões sobre as notificações recebidas semestralmente.

10. As CSIRT ou, se aplicável, as autoridades competentes devem fornecer às autoridades competentes nos termos da Diretiva (UE) 2022/2557 informações sobre os incidentes significativos, os incidentes, as ciberameaças e os quase acidentes notificados nos termos do n.º 1 do presente artigo e do artigo 30.º pelas entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557.

11. A Comissão pode adotar atos de execução que especifiquem o tipo de informações, o formato e o procedimento das notificações apresentadas nos termos do n.º 1 do presente artigo e do artigo 30.º e das comunicações apresentadas nos termos do n.º 2 do presente artigo.

Até 17 de outubro de 2024, a Comissão deve, no que respeita a prestadores de serviços de DNS, aos registos de nomes de TLD, aos prestadores de serviços de computação em nuvem, aos prestadores de serviços de centro de dados, aos fornecedores de redes de distribuição de conteúdos, aos prestadores de serviços geridos, aos prestadores de serviços de segurança geridos, bem como aos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, adotar atos de execução que especifiquem os casos em que um incidente deve ser considerado significativo, conforme referido no n.º 3. A Comissão pode adotar atos de execução em relação a outras entidades essenciais e importantes.

A Comissão deve proceder ao intercâmbio de aconselhamentos e cooperar com o grupo de cooperação sobre os projetos de atos de execução referidos no primeiro e no segundo parágrafos, em conformidade com o artigo 14.º, n.º 4, alínea e).

Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 24.º

Utilização dos sistemas europeus de certificação da cibersegurança

1. A fim de demonstrar o cumprimento de certos requisitos estabelecidos no artigo 21.º, os Estados-Membros podem exigir que as entidades essenciais e importantes utilizem determinados produtos de TIC, serviços de TIC e processos de TIC, desenvolvidos pela entidade essencial ou importante ou fornecidos por terceiros, que estejam certificados no âmbito de sistemas europeus de certificação da cibersegurança adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881. Além disso, os Estados-Membros devem incentivar as entidades essenciais e importantes a utilizar serviços de confiança qualificados.

2. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 38.º para completar a presente diretiva, especificando as categorias de entidades essenciais e importantes obrigadas a utilizar produtos de TIC, serviços de TIC e processos de TIC certificados ou a obter um certificado ao abrigo de um sistema europeu de cibersegurança adotado nos termos do artigo 49.º do Regulamento (UE) 2019/881. Esses atos delegados devem ser adotados sempre que sejam identificados níveis insuficientes de cibersegurança e devem incluir um período de execução.

Antes de adotar esses atos delegados, a Comissão deve efetuar uma avaliação de impacto e levar a cabo consultas em conformidade com o artigo 56.º do Regulamento (UE) 2019/881.

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

Artigo 25.º

Normalização

1. A fim de promover a aplicação convergente do artigo 21.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 técnicas europeias e internacionais aplicáveis à segurança dos sistemas de rede e informação.

2. A ENISA deve formular, em cooperação com os Estados-Membros, e, se for caso disso, após consulta das partes interessadas pertinentes, 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, que permitiriam abranger esses domínios.

CAPÍTULO V

COMPETÊNCIA E REGISTO

Artigo 26.º

Competência e territorialidade

1. Considera-se que as entidades abrangidas pelo âmbito de aplicação da presente diretiva estão sob a jurisdição do Estado-Membro em que se encontram estabelecidas, exceto:

a) Os fornecedores de redes públicas de comunicações eletrónicas ou os prestadores de serviços de comunicações eletrónicas acessíveis ao público, que devem ser considerados como estando sob a jurisdição do Estado-Membro em que prestam os seus serviços;

b) Os prestadores de serviços de DNS, os registos de nomes de TLD, as entidades que prestam serviços de registo de nomes de domínio, 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, os prestadores de serviços de segurança geridos, bem como os prestadores de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais, que devem ser considerados como estando sob a jurisdição do Estado-Membro em que têm o seu estabelecimento principal na União, nos termos do n.º 2;

c) As entidades da administração pública, que devem ser consideradas como estando sob a jurisdição do Estado-Membro que as estabeleceu.

2. Para efeitos da presente diretiva, considera-se que uma entidade tal como referida no n.º 1, alínea b), tem 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 não for possível determinar esse Estado-Membro ou se tais decisões não forem tomadas na União, considera-se que o estabelecimento principal se situa no Estado-Membro em que são levadas a cabo as operações de cibersegurança. Se não for possível determinar esse Estado-Membro, considera-se que o estabelecimento principal se situa no Estado-Membro em que a entidade em causa tem o estabelecimento com o maior número de trabalhadores na União.

3. Se uma entidade a que se refere o n.º 1, alínea b), 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 na União designado nos termos do presente número, qualquer Estado-Membro em que a entidade preste serviços pode intentar ações judiciais contra essa entidade por infração à presente diretiva.

4. A designação de um representante por parte de uma entidade a que se refere o n.º 1, alínea b), não prejudica as ações judiciais que possam ser intentadas contra a própria entidade.

5. Os Estados-Membros que tenham recebido um pedido de assistência mútua em relação a uma entidade a que se refere o n.º 1, alínea b), podem, dentro dos limites desse pedido, tomar medidas de supervisão e execução adequadas em relação à entidade em causa que presta serviços ou que tem um sistema de rede e informação no seu território.

Artigo 27.º

Registo de entidades

1. A ENISA deve criar e manter um registo de prestadores de serviços de DNS, registos de nomes de TLD, entidades que prestam serviços de registo de nomes de domínio, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, fornecedores de redes de distribuição de conteúdos, prestadores de serviços geridos, prestadores de serviços de segurança geridos, bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, com base nas informações recebidas dos pontos de contacto únicos em conformidade com o n.º 4. Mediante pedido, a ENISA permite o acesso das autoridades competentes a esse registo, assegurando simultaneamente a proteção da confidencialidade das informações, se aplicável.

2. O mais tardar em 17 de janeiro de 2025, os Estados-Membros exigem que as entidades a que se refere o n.º 1 apresentem as seguintes informações às autoridades competentes:

a) Nome da entidade;

b) Setor, subsetor e tipo de entidade a que se referem o anexo I ou II, se aplicável;

c) Endereço do estabelecimento principal da entidade e dos outros estabelecimentos legais que possui na União ou, se não estiver estabelecida na União, do seu representante designado nos termos do artigo 26.º, n.º 3;

d) Contactos atualizados, incluindo endereços de correio eletrónico e números de telefone da entidade e, se aplicável, do seu representante designado nos termos do artigo 26.º, n.º 3;

e) Estados-Membros onde a entidade presta serviços; e

f) Gamas de endereços IP da entidade.

3. Os Estados-Membros devem assegurar que as entidades referidas no n.º 1 notifiquem a autoridade competente de alterações das informações que forneceram nos termos do n.º 2, sem demora e, em qualquer caso, no prazo de três meses a contar da data da alteração.

4. Após a receção das informações a que se referem os n.os 2 e 3, exceto as referidas no n.º 2, alínea f), o ponto de contacto único do Estado-Membro em causa deve transmitir essas informações à ENISA sem demora injustificada.

5. Se aplicável, as informações a que se referem os n.os 2 e 3 do presente artigo devem ser transmitidas através do mecanismo nacional a que se refere o artigo 3.º, n.º 4, quarto parágrafo.

Artigo 28.º

Base de dados relativos ao registo dos nomes de domínio

1. Com vista a contribuir para a segurança, a estabilidade e a resiliência do DNS, os Estados-Membros devem exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio recolham e mantenham dados exatos e completos relativos ao registo de nomes de domínio numa base de dados específica, com a devida diligência, em conformidade com o direito da União em matéria de proteção de dados no que respeita aos dados pessoais.

2. Para efeitos do n.º 1, os Estados-Membros devem exigir que a base de dados relativos ao registo de nomes de domínio contenha 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 TLD. Essas informações devem incluir:

a) O nome de domínio;

b) A data de registo;

c) O nome, o endereço de correio eletrónico de contacto e o número de telefone do requerente de registo;

d) O endereço de correio eletrónico de contacto e o número de telefone do ponto de contacto que administra o nome de domínio, caso sejam diferentes dos do requerente de registo.

3. Os Estados-Membros devem ainda exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio disponham de políticas e procedimentos, incluindo procedimentos de verificação, para assegurar que as bases de dados a que se refere o n.º 1 contêm informações exatas e completas. Os Estados-Membros devem exigir que essas políticas e procedimentos sejam tornados públicos.

4. Os Estados-Membros devem exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio a esses registos tornem públicos, sem demora injustificada após o registo de um nome de domínio, os dados relativos ao registo de nomes de domínio que não sejam dados pessoais.

5. Os Estados-Membros devem exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio concedam acesso a dados específicos relativos ao registo de nomes de domínio aos requerentes legítimos de acesso que apresentem um pedido lícito e devidamente fundamentado, em conformidade com o direito da União em matéria de proteção de dados. Os Estados-Membros devem exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio respondam sem demora injustificada e, em qualquer caso, no prazo de 72 horas a contar da receção dos pedidos de acesso. Compete aos Estados-Membros exigir que as políticas e os procedimentos de divulgação dos referidos dados sejam tornados públicos.

6. O cumprimento das obrigações previstas nos n.os 1 a 5 não pode resultar numa duplicação da recolha dos dados de registo de nomes de domínio. Para o efeito, os Estados-Membros devem exigir que os registos de nomes de TLD e as entidades que prestam serviços de registo de nomes de domínio cooperem entre si.

CAPÍTULO VI

PARTILHA DE INFORMAÇÕES

Artigo 29.º

Acordos de partilha de informações sobre cibersegurança

1. Os Estados-Membros devem assegurar que as entidades abrangidas pelo âmbito de aplicação da presente diretiva, assim como, quando pertinente, outras entidades não abrangidas pelo âmbito de aplicação da presente diretiva, possam proceder, a título voluntário, ao intercâmbio de informações pertinentes sobre cibersegurança, nomeadamente relacionadas com ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques, desde que tal partilha de informações:

a) Tenha como objetivo evitar, detetar, dar resposta e recuperar de incidentes ou atenuar o seu impacto;

b) Reforce o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação, apoiar um leque de capacidades defensivas, a correção e divulgação de vulnerabilidades, as técnicas de deteção, contenção e prevenção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação, ou promover a investigação colaborativa de ciberameaças entre entidades públicas e privadas.

2. Os Estados-Membros devem assegurar que o intercâmbio de informações ocorre no seio de comunidades de entidades essenciais e importantes e, quando pertinente, dos seus fornecedores ou prestadores de serviços. Tal intercâmbio deve ser executado mediante acordos de partilha de informações sobre cibersegurança que protejam a natureza potencialmente sensível das informações partilhadas.

3. Os Estados-Membros devem facilitar a celebração dos acordos de partilha de informações sobre cibersegurança a que se refere o n.º 2 do presente artigo. Esses acordos podem especificar os elementos operacionais, incluindo a utilização de plataformas TIC dedicadas e de ferramentas de automatização, o teor e as condições dos acordos de partilha de informações. Ao definir os pormenores do envolvimento das autoridades públicas nesses acordos, os Estados-Membros podem impor condições relativamente às informações disponibilizadas pelas autoridades competentes ou pelas CSIRT. Os Estados-Membros devem oferecer assistência à aplicação de tais acordos, em conformidade com as suas políticas a que se refere o artigo 7.º, n.º 2, alínea h).

4. Os Estados-Membros devem velar por que as entidades essenciais e importantes notifiquem as autoridades competentes da sua participação nos acordos de partilha de informações sobre cibersegurança 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 prestar assistência à celebração dos acordos de partilha de informações sobre cibersegurança referidos no n.º 2, procedendo ao intercâmbio de boas práticas e facultando orientações.

Artigo 30.º

Notificação voluntária de informações pertinentes

1. Os Estados-Membros devem assegurar que, para além da obrigação de notificação prevista no artigo 23.º, as notificações possam ser apresentadas às CSIRT ou, se aplicável, às autoridades competentes, a título voluntário, por:

a) Entidades essenciais e importantes em caso de incidentes, ciberameaças e quase incidentes;

b) Entidades que não as referidas na alínea a), independentemente de serem ou não abrangidas pelo âmbito de aplicação da presente diretiva, em caso de incidentes significativos, ciberameaças e quase incidentes.

2. Os Estados-Membros devem tratar as notificações a que se refere o n.º 1 do presente artigo de acordo com o procedimento previsto no artigo 23.º. Os Estados-Membros podem dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias.

Se necessário, as CSIRT e, se aplicável, as autoridades competentes fornecem aos pontos de contacto único as informações sobre as notificações recebidas nos termos do presente artigo, garantindo simultaneamente a confidencialidade e a proteção adequada das informações fornecidas pela entidade notificadora. Sem prejuízo da prevenção, 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.

CAPÍTULO VII

SUPERVISÃO E EXECUÇÃO

Artigo 31.º

Aspetos gerais relativos à supervisão e à execução

1. Os Estados-Membros devem assegurar que as suas autoridades competentes controlam eficazmente o cumprimento da presente diretiva e tomam as medidas necessárias para garantir esse cumprimento.

2. Os Estados-Membros podem autorizar as suas autoridades competentes a dar prioridade a funções de supervisão. Essa prioritização deve basear-se numa abordagem baseada no risco. Para o efeito, no exercício das suas funções de supervisão previstas nos artigos 32.º e 33.º, as autoridades competentes podem estabelecer metodologias de supervisão que permitam hierarquizar essas funções de acordo com uma abordagem baseada no risco.

3. Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita cooperação com as autoridades de supervisão nos termos do Regulamento (UE) 2016/679, sem prejuízo das competências e funções que incumbem às autoridades de supervisão nos termos desse regulamento.

4. Sem prejuízo dos enquadramentos legislativos e institucionais nacionais, os Estados-Membros devem assegurar que, no âmbito da supervisão do cumprimento da presente diretiva pelas entidades da administração pública e da imposição de medidas de execução no que respeita a infrações à presente diretiva, as autoridades competentes disponham dos poderes adequados para desempenhar essas funções com independência operacional em relação às entidades da administração pública supervisionadas. Os Estados-Membros podem decidir impor medidas de supervisão e execução adequadas, proporcionadas e eficazes em relação a essas entidades, em conformidade com os enquadramentos legislativos e institucionais nacionais.

Artigo 32.º

Medidas de supervisão e execução relativas a entidades essenciais

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

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

a) Inspeções no local e supervisão remota, incluindo controlos aleatórios efetuados por profissionais qualificados;

b) Auditorias de segurança regulares e específicas realizadas por um organismo independente ou por uma autoridade competente;

c) Auditorias ad hoc, incluindo em casos justificados por um incidente significativo ou por infração à presente diretiva por parte da entidade essencial;

d) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa;

e) Pedidos de informações necessárias para avaliar as medidas de gestão dos riscos de cibersegurança adotadas pela entidade em causa, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de apresentar informações às autoridades competentes nos termos do artigo 27.º;

f) Pedidos de acesso a dados, documentos e informações necessárias para o desempenho das 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.

As auditorias de segurança específicas a que se refere o primeiro parágrafo, alínea b), devem basear-se em avaliações de risco realizadas pela autoridade competente ou pela entidade auditada, ou noutras informações disponíveis relacionadas com os riscos.

Os resultados das auditorias de segurança específicas devem ser facultados à autoridade competente. Os custos das auditorias de segurança específicas realizadas por um organismo independente são pagos pela entidade auditada, exceto em casos devidamente fundamentados em que a autoridade competente decida em contrário.

3. Ao exercerem os poderes previstos no n.º 2, alíneas e), f) ou 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 em relação a entidades essenciais, as suas autoridades competentes dispõem de poderes para, pelo menos:

a) Emitir advertências sobre infrações à presente diretiva por parte das entidades em causa;

b) Adotar instruções vinculativas, inclusivamente em relação às medidas necessárias para impedir ou corrigir um incidente, bem como aos prazos para executar essas medidas e para informar sobre a sua execução, ou uma ordem que exija que as entidades em causa corrijam as deficiências detetadas ou as infrações à presente diretiva;

c) Ordenar que as entidades em causa cessem condutas que infrinjam a presente diretiva e se abstenham de as repetir;

d) Ordenar que as entidades em causa garantam que as suas medidas de gestão dos riscos de cibersegurança cumpram o disposto no artigo 21.º ou cumpram as obrigações de notificação estabelecidas no artigo 23.º de uma forma e num período especificados;

e) Ordenar que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou levam a cabo 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 as entidades em causa apliquem, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança;

g) Designar um supervisor com funções bem definidas durante um determinado período para supervisionar o cumprimento pelas entidades em causa dos artigos 21.º e 23.º;

h) Ordenar que as entidades em causa tornem públicos os aspetos das infrações à presente diretiva de uma determinada forma;

i) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, em conformidade com o direito nacional, de uma coima nos termos do artigo 34.º, em complemento de qualquer uma das medidas referidas nas alíneas a) a h) do presente número.

5. Sempre que as medidas de execução adotadas nos termos do n.º 4, alíneas a) a d) e f), se revelarem ineficazes, os Estados-Membros devem assegurar que as suas 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 suas autoridades competentes dispõem de poderes para:

a) Suspender temporariamente ou solicitar a um organismo de certificação ou autorização, ou a um tribunal, em conformidade com o direito nacional, a suspensão temporária de uma certificação ou autorização relativa a uma parte ou à totalidade dos serviços relevantes prestados ou das atividades levadas a cabo pela entidade essencial;

b) Solicitar que os organismos ou tribunais competentes, em conformidade com o direito nacional, proíbam temporariamente qualquer pessoa singular com responsabilidades de gestão a nível de diretor executivo ou de representante legal de exercer funções de gestão nessa entidade essencial.

As suspensões ou proibições temporárias impostas nos termos do presente número só são aplicadas até a entidade em causa tomar as medidas necessárias para corrigir as deficiências ou cumprir os requisitos da autoridade competente responsável pela aplicação dessas medidas de execução. A imposição dessas suspensões ou proibições temporárias deve ser sujeita a garantias processuais adequadas, em conformidade com os princípios gerais do direito da União e da Carta, como o direito a um recurso efetivo e a um processo equitativo, a presunção de inocência e os direitos de defesa.

As medidas de execução 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 legal 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 poder para assegurar o seu cumprimento da presente diretiva. Os Estados-Membros devem assegurar que seja possível considerar essas pessoas singulares responsáveis pela violação dos seus deveres de assegurar o cumprimento da presente diretiva.

No que diz respeito às entidades da administração pública, o presente número é aplicável sem prejuízo do direito nacional em matéria de responsabilidade dos funcionários públicos e dos funcionários eleitos ou nomeados.

7. Ao tomarem qualquer uma das medidas de execução a que se refere o n.º 4 ou 5, as autoridades competentes devem respeitar os direitos de 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, sendo que, em qualquer circunstância, devem ser consideradas infrações graves as seguintes infrações:

   i) violações repetidas,

   ii) não notificação ou não correção de incidentes significativos,

   iii) não correção de deficiências na sequência de instruções vinculativas das autoridades competentes,

   iv) obstrução de auditorias ou atividades de acompanhamento ordenadas pela autoridade competente na sequência da constatação de uma infração,

   v) prestação de informações falsas ou grosseiramente inexatas em relação às medidas de gestão dos riscos de cibersegurança ou às obrigações de notificação estabelecidas nos artigos 21.º e 23.º;

b) A duração da infração;

c) Quaisquer anteriores infrações relevantes cometidas pela entidade em causa;

d) Quaisquer danos materiais ou imateriais causado, incluindo quaisquer prejuízos financeiros ou económicos, os efeitos noutros serviços e o número de utilizadores afetados;

e) Qualquer intenção ou negligência do autor da infração;

f) Quaisquer medidas tomadas pela entidade para prevenir ou atenuar os danos materiais ou imateriais;

g) Qualquer cumprimento de códigos de conduta ou procedimentos de certificação aprovados;

h) 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 de execução. Antes de adotarem tais medidas, as autoridades competentes devem notificar as entidades em causa das suas conclusões preliminares. Devem igualmente conceder um prazo razoável para que essas entidades apresentem as suas observações, exceto em casos devidamente fundamentados em que, de outro modo, seja travada a adoção de medidas imediatas para prevenir ou responder a incidentes.

9. Os Estados-Membros devem assegurar que as suas autoridades competentes nos termos da presente diretiva informam as autoridades competentes no mesmo Estado-Membro nos termos da Diretiva (UE) 2022/2557 no exercício dos seus poderes de supervisão e execução destinados a assegurar o cumprimento da presente diretiva por parte de uma entidade identificada como crítica nos termos da Diretiva 2022/2557. Se for caso disso, as autoridades competentes nos termos da Diretiva (UE) 2022/2557 podem solicitar às autoridades competentes ao abrigo da presente diretiva que exerçam os seus poderes de supervisão e de execução em relação a uma entidade que seja identificada como entidade crítica nos termos da Diretiva (UE) 2022/2557.

10. Os Estados-Membros devem velar por que as suas autoridades competentes nos termos da presente diretiva cooperem com as autoridades competentes relevantes do Estado-Membro em causa nos termos do Regulamento (UE) 2022/2554. Em particular, os Estados-Membros asseguram que as suas autoridades competentes nos termos da presente diretiva informam o Fórum de Fiscalização criado nos termos do artigo 32.º, n.º 1, do Regulamento (UE) 2022/2554 no exercício dos seus poderes de supervisão e execução destinados a assegurar o cumprimento da presente diretiva por parte de uma entidade essencial que seja identificada como um terceiro prestador de serviços no domínio das TIC crítico nos termos do artigo 31.º do Regulamento (UE) 2022/2554.

Artigo 33.º

Medidas de supervisão e execução relativas a entidades importantes

1. Sempre que lhes sejam apresentadas provas, indícios ou informações de que uma entidade importante não está alegadamente a cumprir a presente diretiva, em especial os seus artigos 21.º e 23.º, os Estados-Membros devem assegurar que as autoridades competentes atuam em conformidade, se necessário, tomando medidas de supervisão *ex post*. Os Estados-Membros devem velar por que estas medidas sejam eficazes, 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 importantes, as autoridades competentes dispõem de poderes para submeter essas entidades a, pelo menos:

a) Inspeções no local e supervisão *ex post* remota efetuadas por profissionais qualificados;

b) Auditorias de segurança específicas realizadas por um organismo independente ou por uma autoridade competente;

c) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa;

d) Pedidos de informações necessárias para avaliar *ex post* as medidas de gestão dos riscos de cibersegurança adotadas pela entidade em causa, incluindo políticas de cibersegurança documentadas, bem como o cumprimento da obrigação de apresentar informações às autoridades competentes nos termos do artigo 27.º;

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

f) 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.

As auditorias de segurança específicas a que se refere o primeiro parágrafo, alínea b), devem basear-se em avaliações de risco realizadas pela autoridade competente ou pela entidade auditada, ou noutras informações disponíveis relacionadas com os riscos.

Os resultados das auditorias de segurança específicas devem ser facultados à autoridade competente. Os custos das auditorias de segurança específicas realizadas por um organismo independente são pagos pela entidade auditada, exceto em casos devidamente fundamentados em que a autoridade competente decida em contrário.

3. Ao exercerem os poderes nos termos do n.º 2, alíneas d), e) ou f), 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 em relação a entidades importantes, as autoridades competentes dispõem de poderes para pelo menos:

a) Emitir advertências sobre infrações à presente diretiva por parte das entidades em causa;

b) Adotar instruções vinculativas ou uma ordem que exija que as entidades em causa corrijam as deficiências detetadas ou as infrações à presente diretiva;

c) Ordenar que essas entidades cessem condutas que infrinjam apresente diretiva e se abstenham de as repetir;

d) Ordenar que as entidades em causa garantam que as suas medidas de gestão dos riscos de cibersegurança cumpram o disposto no artigo 21.º ou cumpram as obrigações de notificação estabelecidas no artigo 23.º de uma forma e num período especificados;

e) Ordenar que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou levam a cabo 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 singulares ou coletivas em resposta a essa ameaça;

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

g) Ordenar que essas entidades tornem públicos os aspetos das infrações à presente diretiva de uma determinada forma;

h) Impor ou solicitar a imposição, por parte dos organismos ou tribunais competentes, em conformidade com o direito nacional, de uma coima nos termos do artigo 34.º, em complemento de qualquer uma das medidas referidas nas alíneas a) a g) do presente número.

5. O artigo 32.º, n.ºs 6, 7 e 8, aplica-se *mutatis mutandis* às medidas de supervisão e de execução previstas no presente artigo relativas às entidades importantes.

6. Os Estados-Membros devem velar por que as suas autoridades competentes nos termos da presente diretiva cooperem com as autoridades competentes relevantes do Estado-Membro em causa nos termos do Regulamento (UE) 2022/2554. Em particular, os Estados-Membros asseguram que as suas autoridades competentes nos termos da presente diretiva informam o Fórum de Fiscalização criado nos termos do artigo 32.º, n.º 1, do Regulamento (UE) 2022/2554 no exercício dos seus poderes de supervisão e execução destinados a assegurar o cumprimento da presente diretiva por parte de uma entidade importante que seja identificada como um terceiro prestador de serviços no domínio das TIC crítico nos termos do artigo 31.º do Regulamento (UE) 2022/2554.

Artigo 34.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, no que respeita às infrações à presente diretiva são efetivas, proporcionadas e dissuasivas, tendo em conta as circunstâncias de cada caso concreto.

2. São impostas coimas em complemento de qualquer das medidas referidas no artigo 32.º, n.º 4, alíneas a) a h), no artigo 32.º, n.º 5, e no artigo 33.º, n.º 4, alíneas a) a g).

3. Ao decidir sobre a aplicação de uma coima e sobre o seu montante em cada caso concreto, devem ser tidos em devida consideração, no mínimo, os elementos previstos no artigo 32.º, n.º 7.

4. Os Estados-Membros devem assegurar que, sempre que violem as obrigações previstas no artigo 21.º ou 23.º, as entidades essenciais sejam sujeitas, nos termos dos n.ºs 2 e 3 do presente artigo, a coimas num montante máximo não inferior a 10 000 000 EUR ou num montante máximo não inferior a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade essencial pertence, consoante o montante que for mais elevado.

5. Os Estados-Membros devem assegurar que, sempre que violem o artigo 21.º ou 23.º, as entidades importantes sejam sujeitas, nos termos dos n.os 2 e 3 do presente artigo, a coimas num montante máximo não inferior a 7 000 000 EUR ou num montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade importante pertence, consoante o montante que for mais elevado.

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

7. Sem prejuízo dos poderes das autoridades competentes nos termos dos artigos 32.º e 33.º, os Estados-Membros podem adotar regras para determinar se e em que medida podem ser aplicadas coimas às entidades da administração pública.

8. Quando o sistema jurídico de um Estado-Membro não preveja coimas, esse Estado-Membro deve garantir que o presente artigo pode ser aplicado de modo a que a sanção pecuniária seja proposta pela autoridade de controlo competente e aplicada 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 sanções pecuniárias impostas devem ser efetivas, proporcionadas e dissuasivas. O Estado-Membro notifica a Comissão das disposições que adotar nos termos do presente número até 17 de outubro de 2024 e, sem demora, de qualquer alteração subsequente das mesmas.

Artigo 35.º

Infrações que implicam uma violação de dados pessoais

1. Se as autoridades competentes tiverem conhecimento, durante uma ação de supervisão ou execução, de que a infração das obrigações estabelecidas nos artigos 21.º e 23.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 referidas nos artigos 55.º e 56.º do referido regulamento.

2. Se as autoridades de controlo a que se refere o artigo 55.º ou 56.º do Regulamento (UE) 2016/679 aplicarem uma coima nos termos do artigo 58.º, n.º 2, alínea i), desse regulamento, as autoridades competentes não aplicam uma coima nos termos do artigo 34.º da presente diretiva por uma infração prevista no n.º 1 do presente artigo que resulte do mesmo comportamento que foi objeto da coima nos termos do artigo 58.º, n.º 2, alínea i), do Regulamento (UE) 2016/679. As autoridades competentes podem, no entanto, impor as medidas de execução previstas no artigo 32.º, n.º 4, alíneas a) a h), no artigo 32.º, n.º 5, e no artigo 33.º, n.º 4, alíneas a) a g) 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 deve informar a autoridade de controlo estabelecida no seu próprio Estado-Membro acerca da eventual violação de dados pessoais referida no n.º 1.

Artigo 36.º

Sanções

Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação das disposições nacionais adotadas nos termos da presente diretiva e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Os Estados-Membros notificam a Comissão, até 17 de janeiro de 2025, dessas regras e dessas medidas e também, sem demora, de qualquer alteração ulterior.

Artigo 37.º

Assistência mútua

1. Se uma entidade prestar serviços em mais do que um Estado-Membro, ou prestar serviços em um ou mais Estados-Membros e os seus sistemas de rede e informação estiverem situados noutro ou noutros Estados-Membros, as autoridades competentes dos Estados-Membros 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 de execução 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 de execução tomadas;

b) Uma autoridade competente possa solicitar a outra autoridade competente que tome medidas de supervisão ou de execução;

c) Uma autoridade competente, ao receber um pedido fundamentado de outra autoridade competente, preste à mesma assistência mútua, proporcional aos recursos de que dispõe, para que as medidas de supervisão ou de execução possam ser executadas de forma eficaz, eficiente e coerente.

A assistência mútua referida no primeiro parágrafo, alínea c), 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 se determine que não tem competência para prestar a assistência solicitada, que a assistência solicitada não é proporcionada às funções de supervisão da autoridade competente, ou que o pedido diz respeito a informações ou comporta atividades que, se fossem divulgadas ou realizadas, seriam contrárias aos interesses essenciais do Estado-Membro em matéria de segurança nacional, segurança pública ou defesa. Antes de recusar esse pedido, a autoridade competente consulta as outras autoridades competentes em causa, bem como, a pedido de um dos Estados-Membros interessados, a Comissão e a ENISA.

2. Se for caso disso e de comum acordo, as autoridades competentes de diferentes Estados-Membros podem realizar ações de supervisão conjuntas.

CAPÍTULO VIII

ATOS DELEGADOS E ATOS DE EXECUÇÃO

Artigo 38.º

Exercício da delegação

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

2. O poder de adotar atos delegados referido no artigo 24.º, n.º 2, é conferido à Comissão por um prazo de cinco anos a contar de 16 de janeiro de 2023.

3. A delegação de poderes referida no artigo 24.º, n.º 2 pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

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

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

6. Os atos delegados adotados nos termos do artigo 24.º, n.º 2, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 39.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.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Artigo 40.º

Avaliação

Até 17 de outubro de 2027, e, subsequentemente, a intervalos de 36 meses, a Comissão avalia a aplicação da presente diretiva e apresenta um relatório ao Parlamento Europeu e ao Conselho. O relatório avalia, em particular, a pertinência da dimensão das entidades em causa e dos setores, dos subsetores e dos tipos de entidades referidas nos anexos I e II para o funcionamento da economia e da sociedade no que diz respeito à cibersegurança. Para esse efeito, e a fim de promover a cooperação estratégica e operacional, a Comissão tem em conta os relatórios do grupo de cooperação e da rede de CSIRT sobre a experiência adquirida a nível estratégico e operacional. O relatório deve ser acompanhado, se necessário, de uma proposta legislativa.

Artigo 41.º

Transposição

1. Os Estados-Membros devem adotar e publicar, até 17 de outubro de 2024, as disposições necessárias para dar cumprimento à presente diretiva. Do facto informam imediatamente a Comissão.

Os Estados-Membros devem aplicar essas disposições a partir de 18 de outubro de 2024.

2. As disposições adotadas pelos Estados-Membros a que se refere o n.º 1 devem fazer referência à presente diretiva ou devem ser acompanhadas dessa referência aquando da sua publicação oficial. Os Estados-Membros estabelecem o modo como deve ser feita a referência.

Artigo 42.º

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

No Regulamento (UE) n.º 910/2014, é suprimido o artigo 19.º com efeitos a partir de 18 de outubro de 2024.

Artigo 43.º

Alteração da Diretiva (UE) 2018/1972

Na Diretiva (UE) 2018/1972, são suprimidos os artigos 40.º e 41.º com efeitos a partir de 18 de outubro de 2024.

Artigo 44.º

Revogação

A Diretiva (UE) 2016/1148 é revogada com efeitos a partir de 18 de outubro de 2024.

As remissões para a diretiva revogada devem entender-se como remissões para a presente diretiva e devem ser lidas de acordo com a tabela de correspondência constante do anexo III.

Artigo 45.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 46.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Estrasburgo, em 14 de dezembro de 2022.

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*
R. METSOLA	M. BEK

ANEXO I

SETORES DE IMPORTÂNCIA CRÍTICA

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 do Parlamento Europeu e do Conselho ([1]), que exercem a atividade de «comercialização» na aceção do artigo 2.º, ponto 12, da mesma diretiva
		— 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 do Parlamento Europeu e do Conselho ([2]) — Participantes no mercado 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 59, da Diretiva (UE) 2019/944 — Os operadores de um ponto de carregamento que são responsáveis pela gestão e operação de um ponto de carregamento que presta um serviço de carregamento aos utilizadores finais, incluindo em nome e por conta de um prestador de serviços de mobilidade
	b) Sistemas de aquecimento e arrefecimento urbano	— Operadores de sistemas de aquecimento urbano ou sistemas de arrefecimento urbano na aceção do artigo 2.º, ponto 19, da Diretiva (UE) 2018/2001 do Parlamento Europeu e do Conselho ([3])
	c) Petróleo	— Operadores de oleodutos de petróleo
		— Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
		— Entidades centrais de armazenagem na aceção do artigo 2.º, alínea f), da Diretiva 2009/119/CE do Conselho ([4])
	d) Gás	— Empresas de comercialização na aceção do artigo 2.º, ponto 8, da Diretiva 2009/73/CE do Parlamento Europeu e do Conselho ([5])
		— 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 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

Setor	Subsetor	Tipo de entidade
2. Transportes	a) Transporte aéreo	— Transportadoras aéreas na aceção do artigo 3.º, ponto 4, do Regulamento (CE) n.º 300/2008 utilizadas para fins comerciais
		— Entidades gestoras aeroportuárias na aceção do artigo 2.º, ponto 2, da Diretiva 2009/12/CE do Parlamento Europeu e do Conselho ([6]), aeroportos na aceção do artigo 2.º, ponto 1 da mesma diretiva, incluindo os aeroportos principais enumerados no anexo II, secção 2, do Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho ([7]), e as entidades que exploram instalações auxiliares existentes dentro dos aeroportos
		— 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 do Parlamento Europeu e do Conselho ([8])
	b) Transporte ferroviário	— Gestores de infraestrutura na aceção do artigo 3.º, ponto 2, da Diretiva 2012/34/UE do Parlamento Europeu e do Conselho ([9])
		— Empresas ferroviárias na aceção do artigo 3.º, ponto 1, da Diretiva 2012/34/UE, incluindo os operadores das instalações de serviço na aceção do artigo 3.º, ponto 12, dessa diretiva
	c) Transporte aquático	— Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, tal como definidas para o transporte marítimo no anexo I do Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho ([10]), não incluindo os navios explorados por essas companhias
		— Entidades gestoras dos portos na aceção do artigo 3.º, ponto 1, da Diretiva 2005/65/CE do Parlamento Europeu e do Conselho ([11]), 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 existentes dentro dos portos
		— Operadores de serviços de tráfego marítimo (VTS, do inglês, *vessel traffic services*) na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho ([12])
	d) Transporte rodoviário	— Autoridades rodoviárias na aceção do artigo 2.º, ponto 12, do Regulamento Delegado (UE) 2015/962 ([13]) da Comissão, responsáveis pelo controlo da gestão do tráfego, com exceção das entidades públicas nas quais a gestão do tráfego ou a gestão de sistemas de transporte inteligentes constituem 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 do Parlamento Europeu e do Conselho ([14])
3. Setor bancário		Instituições de crédito, tal como definidas no artigo 4.º, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho ([15])
4. Infraestruturas do mercado financeiro		— Operadores de plataformas de negociação na aceção do artigo 4.º, ponto 24, da Diretiva 2014/65/UE do Parlamento Europeu e do Conselho ([16])
		— Contrapartes centrais (CCP) na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho ([17])

Setor	Subsetor	Tipo de entidade
5. Saúde		— Prestadores de cuidados de saúde na aceção do artigo 3.º, alínea g), da Diretiva 2011/24/UE do Parlamento Europeu e do Conselho ([18])
		— Laboratórios de referência da UE referidas no artigo 15.º do Regulamento (UE) …/… do Parlamento Europeu e do Conselho ([19])
		— Entidades que realizam atividades de investigação e desenvolvimento de medicamentos na aceção do artigo 1.º, ponto 2, da Diretiva 2001/83/CE do Parlamento Europeu e do Conselho ([20]) — Entidades que fabricam produtos farmacêuticos de base e preparações farmacêuticas referidos na secção C, divisão 21, da NACE Rev. 2 — Entidades que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde pública (lista de dispositivos médicos críticos para a emergência de saúde pública) na aceção do artigo 22.º do Regulamento (UE) 2022/123 do Parlamento Europeu e do Conselho ([21])
6. Água potável		Fornecedores e distribuidores de água destinada ao consumo humano na aceção do artigo 2.º, ponto 1, alínea a), da Diretiva (UE) 2020/2184 do Parlamento Europeu e do Conselho ([22]), excluindo os distribuidores para os quais a distribuição de água para consumo humano constitui uma parte não essencial da sua atividade geral de distribuição de outros produtos de base e mercadorias
7. Águas residuais		Empresas que recolhem, eliminam ou tratam águas residuais urbanas, domésticas ou industriais na aceção do artigo 2.º, pontos 1, 2 e 3, da Diretiva 91/271/CEE ([23]) do Conselho, excluindo as empresas para as quais a recolha, eliminação ou tratamento de águas residuais urbanas, domésticas ou industriais constitui 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 raiz
		— Registos de nomes de TLD
		— Prestadores de serviços de computação em nuvem
		— Prestadores de serviços de centro de dados
		— Fornecedores de redes de distribuição de conteúdos
		— Prestadores de serviços de confiança
		— Fornecedores de redes públicas de comunicações eletrónicas
		— Prestadores de serviços de comunicações eletrónicas acessíveis ao público
9. Gestão de serviços TIC (entre empresas)		— Prestadores de serviços geridos — Prestadores de serviços de segurança geridos

Setor	Subsetor	Tipo de entidade
10. Administração pública		— Entidades da administração pública a nível central, tal como definidas pelos Estados-Membros em conformidade com o direito nacional
		— Entidades da administração pública a nível regional tal como definidas por um Estado-Membro em conformidade com o direito nacional
11. 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

([1]) 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).
([2]) 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).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) Directiva 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).
([7]) Regulamento (UE) n. ° 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. ° 661/2010/UE (JO L 348 de 20.12.2013, p. 1).
([8]) Regulamento (CE) n.° 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).
([9]) Diretiva 2012/34/UE do Parlamento Europeu e do Conselho, de 21 de novembro de 2012 , que estabelece um espaço ferroviário europeu único (reformulação) (JO L 343 de 14.12.2012, p. 32).
([10]) Regulamento (CE) n.° 725/2004 do Parlamento Europeu e do Conselho, de 31 de Março de 2004, relativo ao reforço da protecção dos navios e das instalações portuárias (JO L 129 de 29.4.2004, p. 6).
([11]) Directiva 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).
([12]) Directiva 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 Directiva 93/75/CEE do Conselho (JO L 208 de 5.8.2002, p. 10).
([13]) 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).
([14]) 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).
([15]) Regulamento (UE) n.° 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e que altera o Regulamento (UE) n.° 648/2012 (JO L 176 de 27.6.2013, p. 1).
([16]) 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).
([17]) Regulamento (UE) n.° 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).
([18]) 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).

([19]) Regulamento (UE) 2022/2371 do Parlamento Europeu e do Conselho, de 23 de novembro de 2022, relativo às ameaças transfronteiriças graves para a saúde e que revoga a Decisão n.° 1082/2013/UE (JO L 314 de 6.12.2022, p. 26).

([20]) 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).

([21]) Regulamento (UE) 2022/123 do Parlamento Europeu e do Conselho, de 25 de janeiro de 2022, relativo ao reforço do papel da Agência Europeia de Medicamentos em matéria de preparação e gestão de crises no que diz respeito a medicamentos e dispositivos médicos (JO L 20 de 31.1.2022, p. 1).

([22]) Diretiva (UE) 2020/2184 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2020, relativa à qualidade da água destinada ao consumo humano (JO L 435 de 23.12.2020, p. 1).

([23]) 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).

ANEXO II

OUTROS SETORES CRÍTICOS

Setor	Subsetor	Tipo de entidade
1. Serviços postais e de estafeta		Prestadores de serviços postais na aceção do artigo 2.º, ponto 1-A, da Diretiva 97/67/CE, 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 do Parlamento Europeu e do Conselho ([1]), mas excluindo as empresas para as quais a gestão de resíduos não constitui a atividade económica principal
3. Produção, fabrico e distribuição de produtos químicos		Empresas que realizam a produção de substâncias e a distribuição de substâncias ou misturas, referidas no artigo 3.º, pontos 9 e 14, do Regulamento (CE) n.º 1907/2006 do Parlamento Europeu e do Conselho ([2]) e empresas que realizam a produção de «artigos» na aceção do artigo 3.º, ponto 3, do mesmo regulamento, 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 do Parlamento Europeu e do Conselho ([3]), 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 do Parlamento Europeu e do Conselho ([4]), e entidades que fabricam dispositivos médicos para diagnóstico in vitro na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho ([5]), com exceção das entidades que fabricam dispositivos médicos referidas no anexo I, ponto 5, quinto travessão, da presente diretiva
	b) Fabricação de equipamentos informáticos, equipamentos para comunicação, produtos eletrónicos e óticos	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 26, da NACE Rev. 2
	c) Fabricação de equipamento elétrico	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 27, da NACE Rev. 2
	d) Fabricação 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) Fabricação 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) Fabricação de outro equipamento de transporte	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 30, da NACE Rev. 2

Setor	Subsetor	Tipo de entidade
6. Prestadores de serviços digitais		— Prestadores de serviço de mercados em linha
		— Prestadores de serviço de motores de pesquisa em linha
		— Prestadores de serviço de plataformas de serviços de redes sociais
7. Investigação		Organismos de investigação

([1]) 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).

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

ANEXO III

TABELA DE CORRESPONDÊNCIA

Diretiva (UE) 2016/1148	Presente diretiva
Artigo 1.º, n.º 1	Artigo 1.º, n.º 1
Artigo 1.º, n.º 2	Artigo 1.º, n.º 2
Artigo 1.º, n.º 3	–
Artigo 1.º, n.º 4	Artigo 2.º, n.º 12
Artigo 1.º, n.º 5	Artigo 2.º, n.º 13
Artigo 1.º, n.º 6	Artigo 2.º, n.ºs 6 e 11
Artigo 1.º, n.º 7	Artigo 4.º
Artigo 2.º	Artigo 2.º, n.º 14
Artigo 3.º	Artigo 5.º
Artigo 4.º	Artigo 6.º
Artigo 5.º	–
Artigo 6.º	–
Artigo 7.º, n.º 1	Artigo 7.º, n.ºs 1 e 2
Artigo 7.º, n.º 2	Artigo 7.º, n.º 4
Artigo 7.º, n.º 3	Artigo 7.º, n.º 3
Artigo 8.º, n.ºs 1 a 5	Artigo 8.º, n.ºs 1 a 5
Artigo 8.º, n.º 6	Artigo 13.º, n.º 4
Artigo 8.º, n.º 7	Artigo 8.º, n.º 6
Artigo 9.º, n.ºs 1, 2 e 3	Artigo 10.º, n.ºs 1, 2 e 3
Artigo 9.º, n.º 4	Artigo 10.º, n.º 9
Artigo 9.º, n.º 5	Artigo 10.º, n.º 10
Artigo 10.º, n.ºs 1, 2 e 3, primeiro parágrafo	Artigo 13.º, n.ºs 1, 2 e 3
Artigo 10.º, n.º 3, segundo parágrafo	Artigo 23.º, n.º 9
Artigo 11.º, n.º 1	Artigo 14.º, n.ºs 1 e 2
Artigo 11.º, n.º 2	Artigo 14.º, n.º 3
Artigo 11.º, n.º 3	Artigo 14.º, n.º 4, primeiro parágrafo, alíneas a) a q) e alínea s), e n.º 7
Artigo 11.º, n.º 4	Artigo 14.º, n.º 4, primeiro parágrafo, alínea r), e segundo parágrafo
Artigo 11.º, n.º 5	Artigo 14.º, n.º 8
Artigo 12.º, n.ºs 1 a 5	Artigo 15.º, n.ºs 1 a 5
Artigo 13.º	Artigo 17.º
Artigo 14.º, n.os 1 e 2	Artigo 21.º, n.ºs 1 a 4
Artigo 14.º, n.º 3	Artigo 23.º, n.º 1
Artigo 14.º, n.º 4	Artigo 23.º, n.º 3
Artigo 14.º, n.º 5	Artigo 23.º, n.ºs 5, 6 e 8

Diretiva (UE) 2016/1148	Presente diretiva
Artigo 14.º, n.º 6	Artigo 23.º, n.º 7
Artigo 14.º, n.º 7	Artigo 23.º, n.º 11
Artigo 15.º, n.º 1	Artigo 31.º, n.º 1
Artigo 15.º, n.º 2, primeiro parágrafo, alínea a)	Artigo 32.º, n.º 2, alínea e)
Artigo 15.º, n.º 2, primeiro parágrafo, alínea b)	Artigo 32.º, n.º 2, alínea g)
Artigo 15.º, n.º 2, segundo parágrafo	Artigo 32.º, n.º 3
Artigo 15.º, n.º 3	Artigo 32.º, n.º 4, alínea b)
Artigo 15.º, n.º 4	Artigo 31.º, n.º 3
Artigo 16.º, n.ºs 1 e 2	Artigo 21.º, n.ºs 1 a 4
Artigo 16.º, n.º 3	Artigo 23.º, n.º 1
Artigo 16.º, n.º 4	Artigo 23.º, n.º 3
Artigo 16.º, n.º 5	–
Artigo 16.º, n.º 6	Artigo 23.º, n.º 6
Artigo 16.º, n.º 7	Artigo 23.º, n.º 7
Artigo 16.º, n.os 8 e 9	Artigo 21.º, n.º 5, e artigo 23.º, n.º 11
Artigo 16.º, n.º 10	–
Artigo 16.º, n.º 11	Artigo 2.º, n.ºs 1, 2 e 3
Artigo 17.º, n.º 1	Artigo 33.º, n.º 1
Artigo 17.º, n.º 2, alínea a)	Artigo 32.º, n.º 2, alínea e)
Artigo 17.º, n.º 2, alínea b)	Artigo 32.º, n.º 4, alínea b)
Artigo 17.º, n.º 3	Artigo 37.º, n.º 1, alíneas a) e b)
Artigo 18.º, n.º 1	Artigo 26.º, n.º 1, alínea b), e n.º 2
Artigo 18.º, n.º 2	Artigo 26.º, n.º 3
Artigo 18.º, n.º 3	Artigo 26.º, n.º 4
Artigo 19.º	Artigo 25.º
Artigo 20.º	Artigo 30.º
Artigo 21.º	Artigo 36.º
Artigo 22.º	Artigo 39.º
Artigo 23.º	Artigo 40.º
Artigo 24.º	–
Artigo 25.º	Artigo 41.º
Artigo 26.º	Artigo 45.º
Artigo 27.º	Artigo 46.º
Anexo I, ponto 1	Artigo 11.º, n.º 1
Anexo I, ponto 2, alínea a), subalíneas i) a iv)	Artigo 11.º, n.º 2, alíneas a) a d)

Diretiva (UE) 2016/1148	Presente diretiva
Anexo I, ponto 2, alínea a), subalínea v)	Artigo 11.º, n.º 2, alínea f)
Anexo I, ponto 2, alínea b)	Artigo 11.º, n.º 4
Anexo I, ponto 2, alínea c), subalíneas i) e ii)	Artigo 11.º, n.º 5, alínea a)
Anexo II	Anexo I
Anexo III, pontos 1 e 2	Anexo II, ponto 6
Anexo III, ponto 3	Anexo I, ponto 8