I

(Atos legislativos)

DIRETIVAS

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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Deliberando de acordo com o processo legislativo ordinário ([2]),

Considerando o seguinte:

(1) As redes e os sistemas e serviços de informação desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para as atividades económicas e societais e, em especial, para o funcionamento do mercado interno.

(2) A amplitude, a frequência e o impacto dos incidentes de segurança estão a aumentar e constituem uma importante ameaça para o funcionamento das redes e dos sistemas de informação. Esses sistemas podem igualmente tornar-se um alvo de ações danosas deliberadas destinadas a danificar ou a interromper a operação dos sistemas. Esses incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a confiança dos utilizadores e causar graves prejuízos à economia da União.

(3) As redes e os sistemas de informação e, sobretudo, a Internet desempenham um papel crucial para facilitar a circulação transfronteiriça de mercadorias, de serviços e de pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas, intencionais ou não, e independentemente do local onde ocorram, podem afetar os Estados-Membros, individualmente considerados, e a União no seu conjunto. Por consequência, a segurança das redes e dos sistemas de informação é essencial para o bom funcionamento do mercado interno.

(4) Aproveitando os importantes progressos realizados no âmbito do Fórum Europeu dos Estados-Membros no que diz respeito à promoção de debates e intercâmbios de boas práticas, incluindo a definição de princípios de cooperação europeia em caso de cibercrises, deverá ser criado um grupo de cooperação, constituído por representantes dos Estados-Membros, da Comissão e da Agência da União Europeia para a Segurança das Redes e da

([1]) JO C 271 de 19.9.2013, p. 133.
([2]) Posição do Parlamento Europeu de 13 de março de 2014 (ainda não publicada no Jornal Oficial) e posição do Conselho em primeira leitura de 17 de maio de 2016 (ainda não publicada no Jornal Oficial). Posição do Parlamento Europeu de 6 de julho de 2016 (ainda não publicada no Jornal Oficial).

Informação (ENISA), a fim de apoiar e facilitar a cooperação estratégica entre os Estados-Membros no que respeita à segurança das redes e dos sistemas de informação. Para que esse grupo seja eficaz e inclusivo, é indispensável que todos os Estados-Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de segurança das redes e dos sistemas de informação no seu território. Além disso, os requisitos de segurança e de notificação deverão aplicar-se aos operadores de serviços essenciais e aos prestadores de serviços digitais, a fim de promover uma cultura de gestão dos riscos e de assegurar a comunicação dos incidentes mais graves.

(5) As capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e dos sistemas de informação na União. Os Estados-Membros possuem níveis muito diferentes de preparação, o que conduz a abordagens fragmentadas em toda a União. Esta situação traduz-se num nível desigual de defesa dos consumidores e das empresas e compromete o nível global de segurança das redes e dos sistemas de informação na União. Por sua vez, a inexistência de requisitos mínimos comuns a respeitar pelos operadores de serviços essenciais e pelos prestadores de serviços digitais impossibilita a criação de um mecanismo global e eficaz para a cooperação a nível da União. As universidades e os centros de investigação têm um papel determinante a desempenhar para estimular a investigação, o desenvolvimento e a inovação nessas áreas.

(6) Uma resposta eficaz aos desafios que se colocam à segurança das redes e dos sistemas de informação exige, assim, uma abordagem global a nível da União, que abranja os requisitos mínimos comuns de desenvolvimento de capacidades e de planificação, o intercâmbio de informações, a cooperação e os requisitos comuns de segurança para os operadores de serviços essenciais e para os prestadores de serviços digitais. Contudo, os operadores de serviços essenciais e os prestadores de serviços digitais não estão impedidos de aplicar medidas de segurança mais rigorosas do que as previstas na presente diretiva.

(7) A fim de cobrir todos os incidentes e todos os riscos relevantes, a presente diretiva deverá aplicar-se tanto aos operadores de serviços essenciais como aos prestadores de serviços digitais. No entanto, as obrigações que recaem sobre os operadores de serviços essenciais e sobre os prestadores de serviços digitais não deverão aplicar-se às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho ([1]), que estão sujeitas aos requisitos específicos de segurança e integridade estabelecidos na referida diretiva, nem aos prestadores de serviços de confiança na aceção do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([2]), que estão sujeitos aos requisitos de segurança estabelecidos nesse regulamento.

(8) A presente diretiva deverá ser interpretada sem prejuízo da possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos interesses essenciais da sua própria segurança, proteger a ordem e a segurança públicas e para permitir a investigação, a deteção e a repressão das infrações penais. Nos termos do artigo 346.º do Tratado sobre o Funcionamento da União Europeia (TFUE), nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança. São relevantes neste contexto a Decisão 2013/488/UE do Conselho ([3]) e os acordos de não divulgação ou os acordos de não divulgação informais, tais como o protocolo «sinalização luminosa» para a partilha de informações não classificadas (*Information Sharing Traffic Light Protocol*).

(9) Determinados setores da economia são já regulamentados, ou podem vir a ser regulamentados no futuro por atos jurídicos da União de âmbito setorial que incluam regras relacionadas com a segurança das redes e dos sistemas de informação. Sempre que esses atos jurídicos da União contenham disposições que imponham requisitos de segurança das redes e dos sistemas de informação ou de notificação de incidentes, essas disposições deverão aplicar-se se incluírem requisitos que tenham, no mínimo, efeitos equivalentes às obrigações contidas na presente diretiva. Os Estados-Membros deverão então aplicar as disposições desses atos jurídicos da União de âmbito setorial, nomeadamente as relativas à competência, e não deverão levar a cabo o processo de identificação dos operadores de serviços essenciais na aceção da presente diretiva. Neste contexto, os Estados-Membros deverão fornecer à Comissão informações sobre a aplicação de tal *lex specialis*. Para determinar se os requisitos relativos à segurança das redes e dos sistemas de informação e à notificação de incidentes previstos nos atos jurídicos da União de âmbito setorial são equivalentes aos que constam da presente diretiva, deverão ser tidas em consideração apenas as disposições dos atos jurídicos relevantes da União e a sua aplicação nos Estados-Membros.

(10) No setor do transporte marítimo e por vias navegáveis interiores, os requisitos de segurança aplicáveis às empresas, navios, instalações portuárias, portos e serviços de tráfego marítimo ao abrigo de atos jurídicos da União abrangem todas as operações, incluindo os sistemas de rádio e telecomunicações e os sistemas de informação e as redes. Parte dos procedimentos obrigatórios a seguir inclui a notificação de todos os incidentes e, como tal, deverá ser considerada como *lex specialis*, na medida em que esses requisitos sejam, no mínimo, equivalentes às disposições correspondentes da presente diretiva.

([1]) Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (Diretiva-Quadro) (JO L 108 de 24.4.2002, p. 33).

([2]) 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).

([3]) Decisão 2013/488/EU do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 274 de 15.10.2013, p. 1).

(11) Ao identificarem operadores do setor do transporte marítimo e por vias navegáveis interiores, os Estados-Membros deverão ter em conta os códigos e as orientações internacionais — atuais e futuros — elaborados pela Organização Marítima Internacional, a fim de permitir que os diversos operadores marítimos sigam uma abordagem coerente.

(12) A regulamentação e a supervisão nos setores da banca e das infraestruturas dos mercados financeiros estão bastante harmonizadas a nível da União por via do direito primário e do direito derivado da União e das normas elaboradas em conjunto com as autoridades europeias de supervisão. No quadro da União Bancária, a aplicação e supervisão desses requisitos é assegurada pelo Mecanismo Único de Supervisão. Nos Estados-Membros que não fazem parte da União Bancária, tal aplicação e supervisão são asseguradas pelas entidades reguladoras bancárias competentes em cada um deles. Noutras áreas da regulamentação do setor financeiro, o Sistema Europeu de Supervisão Financeira também assegura um elevado grau de uniformização e convergência das práticas de supervisão. A Autoridade Europeia dos Valores Mobiliários e dos Mercados desempenha também um papel de supervisão direta de determinadas entidades, a saber, as agências de notação de risco e os repositórios de transações.

(13) O risco operacional constitui uma parte essencial da regulamentação e supervisão prudenciais nos setores da banca e das infraestruturas dos mercados financeiros. Abrange todas as operações, incluindo a segurança, integridade e resiliência das redes e dos sistemas de informação. Os requisitos relativos a esses sistemas, que frequentemente extravasam os requisitos previstos na presente diretiva, são estabelecidos numa série de atos jurídicos da União, inclusive nas regras aplicáveis ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento e nas regras relativas aos requisitos prudenciais aplicáveis às instituições de crédito e às empresas de investimento, que incluem requisitos relativos ao risco operacional; nas regras aplicáveis aos mercados de instrumentos financeiros, que incluem requisitos relativos à avaliação dos riscos das empresas de investimento e dos mercados regulamentados; nas regras aplicáveis aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, que incluem requisitos relativos ao risco operacional das contrapartes centrais e dos repositórios de transações; e, nas regras aplicáveis à melhoria do sistema de liquidação de valores mobiliários na União e às centrais de depósito de títulos, que incluem requisitos relativos ao risco operacional. Além disso, os requisitos de notificação de incidentes, que fazem parte das práticas normais de supervisão no setor financeiro, são frequentemente incluídos nos manuais de supervisão. Os Estados-Membros deverão considerar essas regras e esses requisitos na sua aplicação da *lex specialis*.

(14) Tal como referido pelo Banco Central Europeu no parecer que emitiu em 25 de julho de 2014 ([1]), a presente diretiva não afeta o regime previsto ao abrigo do direito da União, relativo à superintendência dos sistemas de pagamento e de liquidação no Eurosistema. Conviria que as autoridades responsáveis por essa superintendência trocassem experiências em matérias relacionadas com a segurança das redes e dos sistemas de informação com as autoridades competentes nos termos da presente diretiva. O mesmo se aplica aos membros do Sistema Europeu de Bancos Centrais não pertencentes à área do euro que procedem à superintendência dos sistemas de pagamento e de liquidação com base em disposições legislativas e regulamentares nacionais.

(15) Um mercado em linha permite aos consumidores e aos comerciantes celebrarem contratos de venda ou de prestação de serviços por via eletrónica com comerciantes, e constitui o destino final da celebração desses contratos. O mercado em linha não deverá abranger os serviços prestados por via eletrónica que apenas servem de intermediário para os serviços prestados por terceiros através dos quais, em última análise, o contrato possa ser celebrado. Por conseguinte, não deverá abranger serviços prestados por via eletrónica que comparam o preço de determinados produtos ou serviços de diferentes comerciantes e, em seguida, redirecionam o utilizador para um comerciante preferencial tendo em vista a aquisição do produto. Os serviços de computação fornecidos pelo mercado em linha podem incluir o processamento de transações, a agregação de dados ou a definição de perfis de utilizadores. As lojas de aplicações em linha, que funcionam como lojas em linha que permitem a distribuição digital de aplicações ou de programas informáticos de terceiros, deverão ser entendidas como sendo um tipo de mercado em linha.

(16) Um motor de pesquisa digital permite ao utilizador consultar, em princípio, todos os sítios *web* com base em pesquisas sobre qualquer assunto. Pode, em alternativa, centrar-se em sítios *web* numa determinada língua. A definição de motor de pesquisa em linha dada na presente diretiva não deverá abranger as funções de pesquisa que se limitam ao conteúdo de um sítio *web* específico, independentemente de a função de pesquisa ser ou não fornecida por um motor de pesquisa externo. Também não deverá abranger os serviços prestados por via eletrónica que comparam o preço de determinados produtos ou serviços de diferentes comerciantes e, em seguida, redirecionam o utilizador para um comerciante preferencial tendo em vista a aquisição do produto.

(17) Os serviços de computação em nuvem são muito diversificados e podem ser fornecidos segundo diferentes modelos. Para efeitos da presente diretiva, a expressão «serviços de computação em nuvem» abrange serviços que permitem o acesso a um conjunto modulável e adaptável de recursos de computação partilháveis. Esses recursos de computação incluem recursos como redes, servidores ou outras infraestruturas, armazenamento, aplicações e serviços. O termo «modulável» refere-se a recursos de computação atribuídos de forma flexível pelo prestador de

([1]) JO C 352 de 7.10.2014, p. 4.

serviços de computação em nuvem, independentemente da localização geográfica dos recursos, a fim de fazer face às flutuações da procura. A expressão «conjunto adaptável» é utilizada para descrever os recursos de computação disponibilizados e libertados em função da procura, a fim de aumentar ou diminuir rapidamente os recursos disponíveis, consoante o volume de trabalho. O termo «partilhável» é utilizado para descrever os recursos de computação fornecidos a múltiplos utilizadores que partilham um acesso comum ao serviço mas cujo tratamento é efetuado separadamente para cada utilizador, embora o serviço seja prestado a partir do mesmo equipamento eletrónico.

(18) A função de um ponto de troca de tráfego (*Internet Exchange Point*) consiste em interligar redes. Os pontos de troca de tráfego não proporcionam o acesso às redes nem atuam como prestadores ou operadores de tráfego. Os pontos de troca de tráfego também não prestam outros serviços não relacionados com interligação, embora isso não impeça o operador de um ponto de troca de tráfego de prestar também serviços não conexos. Os pontos de troca de tráfego existem para interligar redes que estejam separadas em termos técnicos e organizativos. A expressão «sistema autónomo» é utilizada para descrever uma rede autónoma do ponto de vista técnico.

(19) Os Estados-Membros deverão ser responsáveis por determinar as entidades que preenchem os critérios da definição de operador de serviços essenciais. A fim de garantir uma abordagem coerente, a definição de operador de serviços essenciais deverá ser aplicada de forma coerente por todos os Estados-Membros. Para esse efeito, a presente diretiva prevê a avaliação das entidades ativas em setores e subsetores específicos, a elaboração de uma lista de serviços essenciais, a análise de uma lista comum dos fatores transetoriais a fim de determinar se um potencial incidente teria um efeito perturbador importante, um processo de consulta que envolva os Estados-Membros pertinentes no caso de haver entidades que prestem serviços em mais de um Estado-Membro, e o apoio do grupo de cooperação no processo de identificação. A fim de garantir que as eventuais alterações no mercado sejam refletidas com exatidão, a lista dos operadores identificados deverá ser revista regularmente pelos Estados-Membros e atualizada sempre que necessário. Por último, os Estados-Membros deverão prestar as informações necessárias à Comissão para que esta possa avaliar em que medida esta metodologia comum lhes permitiu aplicar coerentemente a definição.

(20) No processo de identificação dos operadores de serviços essenciais, os Estados-Membros deverão avaliar, pelo menos para cada um dos subsetores referidos na presente diretiva, os serviços que deverão ser considerados essenciais para a manutenção de atividades societais e económicas cruciais, e se as entidades incluídas nos setores e subsetores a que se refere a presente diretiva e que prestam esses serviços satisfazem os critérios para a identificação dos operadores. Ao avaliar se uma entidade presta um serviço essencial para a manutenção de atividades societais ou económicas cruciais, basta examinar se essa entidade presta um serviço incluído na lista de serviços essenciais. Além disso, deverá demonstrar-se que a prestação desse serviço essencial depende das redes e dos sistemas de informação. Finalmente, ao avaliar se um incidente terá um efeito perturbador importante na prestação do serviço, os Estados-Membros deverão ter em conta vários fatores transetoriais, bem como fatores específicos de cada setor, quando pertinente.

(21) A fim de identificar os operadores de serviços essenciais, o seu estabelecimento num Estado-Membro pressupõe o exercício efetivo e real de uma atividade com base numa organização estável. A forma jurídica dessa organização, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é o fator determinante neste contexto.

(22) É possível que as entidades que operam nos setores e subsetores a que se refere a presente diretiva prestem serviços essenciais e não essenciais. Por exemplo, no setor do transporte aéreo, os aeroportos prestam serviços que podem ser considerados essenciais por um Estado-Membro, tais como a gestão das pistas, mas também uma série de serviços que podem ser considerados não essenciais, como a disponibilização de áreas comerciais. Os operadores de serviços essenciais deverão estar sujeitos aos requisitos de segurança específicos apenas no que respeita aos serviços considerados essenciais. Por conseguinte, a fim de identificar os operadores, os Estados-Membros deverão elaborar uma lista dos serviços que são considerados essenciais.

(23) A lista de serviços deverá incluir todos os serviços prestados no território de um determinado Estado-Membro que preencham os requisitos previstos na presente diretiva. Os Estados-Membros deverão poder complementar a lista existente mediante a inclusão de novos serviços. A lista de serviços deverá servir de ponto de referência para os Estados-Membros, permitindo a identificação dos operadores de serviços essenciais. O seu objetivo é identificar quais são os tipos de serviços essenciais em cada setor a que se refere a presente diretiva, distinguindo-os, assim, das atividades não essenciais pelas quais uma entidade ativa num determinado setor possa ser responsável. A lista de serviços elaborada por cada Estado-Membro serviria de contributo adicional na avaliação das práticas de regulação de cada Estado-Membro com vista a assegurar a coerência global do processo de identificação entre os Estados-Membros.

(24) Para efeitos do processo de identificação, sempre que uma entidade preste um serviço essencial em dois ou mais Estados-Membros, estes deverão proceder a debates bilaterais ou multilaterais entre si. Este processo de consulta destina-se a assisti-los na avaliação da natureza crítica do operador em termos de impacto transfronteiriço, permitindo assim a cada Estado-Membro envolvido apresentar a sua opinião sobre os riscos associados aos serviços prestados. Os Estados-Membros em causa deverão ter em conta a opinião de cada um e deverão poder solicitar a assistência do grupo de cooperação a este respeito.

(25) Em resultado do processo de identificação, os Estados-Membros deverão adotar medidas nacionais para determinar quais as entidades sujeitas a obrigações em matéria de segurança das redes e dos sistemas de informação. Este resultado poderá ser alcançado através da adoção de uma lista que enumere todos os operadores de serviços essenciais ou da adoção de medidas nacionais que incluam critérios objetivos quantificáveis, tais como a produção do operador ou o número de utilizadores, o que permitirá determinar as entidades que estão sujeitas a obrigações em matéria de segurança das redes e dos sistemas de informação. As medidas nacionais, existentes ou adotadas no âmbito da presente diretiva, deverão incluir todas as medidas jurídicas, administrativas e políticas que permitam a identificação dos operadores de serviços essenciais ao abrigo da presente diretiva.

(26) A fim de dar uma indicação da importância dos operadores de serviços essenciais identificados em relação ao setor em causa, os Estados-Membros deverão ter em conta o número e a dimensão desses operadores, por exemplo, em termos de quota de mercado ou da quantidade produzida ou transportada, sem serem obrigados a divulgar informações suscetíveis de revelar os operadores identificados.

(27) A fim de determinar se um incidente pode ter um efeito perturbador importante na prestação de um serviço essencial, os Estados-Membros deverão ter em conta diversos fatores, nomeadamente o número de utilizadores que dependem desse serviço para fins privados ou profissionais. A utilização desse serviço pode ser direta, indireta ou por intermediação. Ao avaliar o impacto que um incidente poderá ter, em termos de intensidade e duração, nas atividades económicas e societais ou na segurança pública, os Estados-Membros deverão avaliar igualmente o tempo que pode decorrer antes de a descontinuidade começar a ter um impacto negativo.

(28) Além dos fatores transetoriais, também deverão ser tidos em conta os fatores específicos do setor a fim de determinar se um incidente pode ter um efeito perturbador importante na prestação de um serviço essencial. No que diz respeito aos fornecedores de energia, esses fatores poderão incluir a quantidade ou a percentagem de energia nacional gerada; para os fornecedores de petróleo, o volume diário; para o transporte aéreo, incluindo os aeroportos e as transportadoras aéreas, o transporte ferroviário e os portos marítimos, a percentagem de volume de tráfego nacional e o número de passageiros ou de operações de movimentação de carga anuais; para os serviços bancários ou as infraestruturas do mercado financeiro, a sua importância sistémica com base nos ativos totais ou no rácio ativos totais/PIB; para o setor da saúde, o número de pacientes sob cuidados do prestador em cada ano; para a produção, tratamento e fornecimento de água, o volume, o número e os tipos de utilizadores aos quais a água é fornecida, incluindo, por exemplo, hospitais, serviços públicos, organizações ou particulares e a existência de fontes alternativas de abastecimento de água que abranjam a mesma zona geográfica.

(29) A fim de atingir e manter um nível elevado de segurança das redes e dos sistemas de informação, cada Estado-Membro deverá dispor de uma estratégia nacional de segurança das redes e dos sistemas de informação que defina os objetivos estratégicos e as ações estratégicas concretas a executar.

(30) 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, bem como evitar duplicações, os Estados-Membros deverão poder designar mais do que uma autoridade nacional competente responsável pelo desempenho de funções associadas à segurança das redes e dos sistemas de informação dos operadores de serviços essenciais e dos prestadores de serviços digitais, nos termos da presente diretiva.

(31) A fim de facilitar a cooperação e a comunicação transfronteiriça e permitir a aplicação eficaz da presente diretiva, é necessário que cada Estado-Membro designe, sem prejuízo de acordos regulamentares setoriais, um ponto de contacto único nacional responsável pela coordenação das questões relativas à segurança das redes e dos sistemas de informação e pela cooperação transfronteiriça a nível da União. As autoridades competentes e os pontos de contacto únicos deverão dispor de recursos técnicos, financeiros e humanos adequados para garantir a execução eficaz e eficiente das atribuições que lhes são conferidas e para alcançar assim os objetivos da presente diretiva. Dado que a presente diretiva visa melhorar o funcionamento do mercado interno através da criação de um clima de confiança, os organismos dos Estados-Membros deverão estar em condições de cooperar eficazmente com os agentes económicos e estar estruturados em conformidade.

(32) As autoridades competentes ou as equipas de resposta a incidentes de segurança informática (CSIRT) deverão receber notificações de incidentes. Os pontos de contacto únicos não deverão receber diretamente notificações de incidentes, exceto se atuarem também como autoridades competentes ou como CSIRT. No entanto, uma autoridade competente ou uma CSIRT deverá poder encarregar o ponto de contacto único de enviar as notificações de incidentes aos pontos de contacto únicos dos outros Estados-Membros afetados.

(33) A fim de assegurar a prestação efetiva de informações aos Estados-Membros e à Comissão, o ponto de contacto único deverá apresentar ao grupo de cooperação um relatório de síntese anonimizado, a fim de preservar a confidencialidade das notificações e a identidade dos operadores de serviços essenciais e dos prestadores de serviços digitais, uma vez que as informações sobre a identidade das entidades notificadoras não são necessárias para o intercâmbio de boas práticas no grupo de cooperação. O relatório de síntese deverá incluir informações sobre o número de notificações recebidas e indicações sobre a natureza dos incidentes notificados, nomeadamente sobre os tipos de violações da segurança, a sua gravidade ou a sua duração.

(34) Os Estados-Membros deverão estar adequadamente equipados, em termos de capacidade técnica e organizativa, para evitar, detetar e atenuar os incidentes e os riscos ligados às redes e aos sistemas de informação, e para os enfrentar. Por conseguinte, deverão dispor de CSIRT, também conhecidas por equipas de resposta a emergências informáticas (CERT), que funcionem bem e que preencham os requisitos essenciais para garantir capacidades efetivas e compatíveis para fazer face aos incidentes e aos riscos e para assegurar uma cooperação eficaz a nível da União. A fim de que todos os tipos de operadores de serviços essenciais e de prestadores de serviços digitais beneficiem dessas capacidades e dessa cooperação eficaz, os Estados-Membros deverão assegurar que todos eles sejam abrangidos por uma CSIRT designada. 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.

(35) Uma vez que a maioria das redes e dos sistemas de informação são explorados pelo setor privado, a cooperação entre o setor público e setor privado é essencial. Os operadores de serviços essenciais e os prestadores de serviços digitais deverão ser incentivados a criar os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e dos sistemas de informação. Sempre que necessário, o grupo de cooperação deverá poder convidar as partes interessadas relevantes para os debates. Para incentivar efetivamente a partilha de informações e de boas práticas, é essencial assegurar que os operadores de serviços essenciais e os prestadores de serviços digitais que participam nos referidos intercâmbios não fiquem em desvantagem devido à sua cooperação.

(36) A ENISA deverá assistir os Estados-Membros e a Comissão através da disponibilização de competências especializadas e aconselhamento e da facilitação do intercâmbio de boas práticas. Em particular, na aplicação da presente diretiva, a Comissão deverá consultar a ENISA e os Estados-Membros deverão poder fazê-lo. A fim de reforçar as capacidades e os conhecimentos dos Estados-Membros, o grupo de cooperação deverá também servir de instrumento para o intercâmbio de boas práticas e a discussão das capacidades e do grau de preparação dos Estados-Membros e, numa base voluntária, para assistir os seus membros na avaliação das estratégias nacionais de segurança das redes e dos sistemas de informação, no reforço das suas capacidades e na avaliação de exercícios de segurança das redes e dos sistemas de informação.

(37) Sempre que adequado, os Estados-Membros deverão poder utilizar ou adaptar as estruturas organizativas ou as estratégias existentes na aplicação da presente diretiva.

(38) As atribuições do grupo de cooperação e da ENISA são interdependentes e complementares. De um modo geral, a ENISA deverá apoiar o grupo de cooperação na execução das suas atribuições, em consonância com o objetivo da ENISA, definido no Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho ([1]), a saber, prestar assistência às instituições, aos órgãos, aos organismos e às agências da União e aos Estados-Membros na execução das políticas necessárias para respeitar os requisitos legais e regulamentares de segurança das redes e dos sistemas de informação nos termos dos atos jurídicos atuais e futuros da União. A ENISA deverá prestar assistência especialmente nos domínios que correspondem às suas próprias atribuições, tal como definidas no Regulamento (UE) n.º 526/2013, a saber, analisar as estratégias de segurança das redes e dos sistemas de informação, apoiar a organização e a realização de exercícios de segurança das redes e dos sistemas de informação na União, e proceder ao intercâmbio de informações e de boas práticas em matéria de ações de sensibilização e formação. A ENISA deverá igualmente ser envolvida na elaboração de orientações sobre critérios setoriais específicos para determinar a importância do impacto de um incidente.

([1]) Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004 (JO L 165 de 18.6.2013, p. 41).

(39) A fim de promover um grau avançado de segurança das redes e dos sistemas de informação, o grupo de cooperação deverá, sempre que adequado, cooperar com as instituições, os órgãos e os organismos relevantes da União para trocar saber-fazer e boas práticas e prestar aconselhamento sobre aspetos relativos à segurança das redes e dos sistemas de informação que possam ter impacto no seu trabalho, respeitando as disposições existentes em matéria de intercâmbio de informações restritas. Ao cooperar com as autoridades encarregadas da aplicação da lei em aspetos relacionados com a segurança das redes e dos sistemas de informação que possam ter impacto no seu trabalho, o grupo de cooperação deverá respeitar os canais de informação existentes e as redes já criadas.

(40) É cada vez mais importante tanto para o público em geral como para as empresas, em especial para as pequenas e médias empresas, dispor de informações sobre incidentes. Em alguns casos, essas informações são já fornecidas através de sítios *web* a nível nacional e na língua de um país específico, centrando-se principalmente em incidentes e ocorrências de dimensão nacional. Tendo em conta que cada vez mais as empresas operam no plano transfronteiriço e os cidadãos utilizam serviços prestados por via eletrónica, as informações sobre os incidentes ocorridos deverão ser fornecidas de uma forma agregada a nível da União. O secretariado da rede de CSIRT é incentivado a manter um sítio *web* ou a dedicar uma página especial num sítio *web* existente, em que sejam facultadas ao grande público informações gerais sobre os principais incidentes ocorridos na União, tendo em especial atenção os interesses e as necessidades das empresas. As equipas que participam na rede de CSIRT são exortadas a fornecer, a título facultativo, informações a publicar nesse sítio *web*, excluindo, informações confidenciais ou sensíveis.

(41) Caso as informações sejam consideradas confidenciais nos termos das regras nacionais e da União em matéria de sigilo comercial, esse sigilo deverá ser assegurado no exercício das atividades e no cumprimento dos objetivos estabelecidos pela presente diretiva.

(42) Os exercícios que simulam cenários de incidente em tempo real são essenciais para avaliar o grau de preparação e de cooperação dos Estados-Membros no que respeita à segurança das redes e dos sistemas de informação. O ciclo de exercícios CyberEurope, coordenado pela ENISA com a participação dos Estados-Membros, constitui um instrumento útil para testar e elaborar recomendações sobre a forma como deverá evoluir o tratamento de incidentes a nível da União ao longo do tempo. Considerando que os Estados-Membros não são atualmente obrigados a planear ou a participar em exercícios, a criação da rede de CSIRT prevista na presente diretiva deverá permitir que os Estados-Membros participem em exercícios com base em planos específicos e em escolhas estratégicas. O grupo de cooperação criado nos termos da presente diretiva deverá discutir as decisões estratégicas respeitantes aos exercícios, em especial — mas não exclusivamente — no que respeita à regularidade da sua realização e à conceção dos cenários. De acordo com o seu mandato, a ENISA deverá apoiar a organização e a realização dos exercícios a nível da União, facultando conhecimentos especializados e prestando aconselhamento ao grupo de cooperação e à rede de CSIRT.

(43) Atendendo ao caráter global dos problemas de segurança que afetam as redes e os sistemas de informação, é necessário estreitar a cooperação internacional para melhorar as normas de segurança e o intercâmbio de informações e promover uma abordagem comum global das questões de segurança.

(44) A responsabilidade de garantir a segurança das redes e dos sistemas de informação cabe, em larga medida, aos operadores de serviços essenciais e aos prestadores de serviços digitais. Dever-se-á promover e desenvolver uma cultura de gestão de riscos que passe pela avaliação dos riscos e pela aplicação de medidas de segurança adequadas aos riscos enfrentados, estabelecendo para tal requisitos regulamentares adequados e adotando práticas setoriais de caráter voluntário. Criar condições de concorrência dignas de confiança e equitativas é também essencial para que o grupo de cooperação e a rede de CSIRT funcionem com eficácia e para garantir que todos os Estados-Membros cooperem de forma efetiva.

(45) A presente diretiva aplica-se apenas às administrações públicas identificadas como operadores de serviços essenciais. Por conseguinte, cabe aos Estados-Membros garantir a segurança das redes e dos sistemas de informação das administrações públicas que não se insiram no âmbito de aplicação da presente diretiva.

(46) As medidas de gestão de riscos incluem medidas para identificar os riscos de incidentes, para evitar, detetar e gerir os incidentes e para atenuar o seu impacto. A segurança das redes e dos sistemas de informação abrange a segurança dos dados armazenados, transmitidos e tratados.

(47) As autoridades competentes deverão manter a possibilidade de adotar orientações nacionais sobre as circunstâncias em que os operadores de serviços essenciais são obrigados a notificar incidentes.

(48) Muitas das empresas na União dependem dos prestadores de serviços digitais para efeitos de prestação dos seus próprios serviços. Uma vez que alguns serviços digitais poderão constituir um recurso importante para os seus utilizadores, incluindo os operadores de serviços essenciais, e atendendo a que esses utilizadores poderão nem sempre ter alternativas ao seu dispor, a presente diretiva deverá aplicar-se igualmente aos prestadores desses serviços. A segurança, a continuidade e a fiabilidade do tipo de serviços digitais a que se refere a presente diretiva são essenciais para o bom funcionamento de muitas empresas. A ocorrência de uma perturbação num desses serviços digitais pode impedir a prestação de outros serviços que dele dependam e, como tal, pode afetar atividades económicas e societais fundamentais na União. Esses serviços digitais poderão, pois, ser de importância crucial para o bom funcionamento das empresas que deles dependem e, além disso, para a participação dessas empresas no mercado interno e nas trocas comerciais transfronteiriças na União. Esses prestadores de serviços digitais, abrangidos pela presente diretiva, são aqueles que se considera oferecerem serviços digitais dos quais grande parte das empresas da União depende cada vez mais.

(49) Os prestadores de serviços digitais deverão garantir um nível de segurança proporcional ao grau de risco para a segurança dos serviços digitais que fornecem, dada a importância dos seus serviços para as operações de outras empresas na União. Na prática, o grau de risco para os operadores de serviços essenciais, que desempenham muitas vezes um papel crucial para a manutenção de atividades societais e económicas cruciais, é superior ao grau de risco a que os prestadores de serviços digitais estão sujeitos. Por conseguinte, os requisitos de segurança aplicáveis aos prestadores de serviços digitais deverão ser menos exigentes. Os prestadores de serviços digitais deverão continuar a ter a liberdade de tomar as medidas que considerem adequadas para gerir os riscos de segurança que se coloquem às suas redes e aos seus sistemas de informação. Dada a sua vocação transfronteiriça, os prestadores de serviços digitais deverão ser sujeitos a requisitos mais harmonizados a nível da União. Os atos de execução deverão facilitar a especificação e aplicação dessas medidas.

(50) Embora os fabricantes de *hardware* e os responsáveis pelo desenvolvimento de *software* não sejam operadores de serviços essenciais nem prestadores de serviços digitais, os seus produtos reforçam a segurança das redes e dos sistemas de informação. Como tal, desempenham um papel importante ao permitirem que os operadores de serviços essenciais e os prestadores de serviços digitais protejam as suas redes e dos seus sistemas de informação. Esses produtos de *hardware* e *software* já estão sujeitos às regras existentes em matéria de responsabilidade pelos produtos.

(51) As medidas técnicas e organizativas impostas aos operadores de serviços essenciais e aos prestadores de serviços digitais não deverão exigir que um determinado produto das tecnologias da informação e da comunicação que tenha fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico.

(52) Os operadores de serviços essenciais e os prestadores de serviços digitais deverão garantir a segurança das redes e dos sistemas de informação que utilizam. Trata-se principalmente de redes e sistemas de informação privados geridos por pessoal interno especializado em TI ou cuja segurança tenha sido externalizada. Os requisitos de segurança e notificação deverão aplicar-se aos operadores de serviços essenciais e aos prestadores de serviços digitais relevantes, independentemente do facto de estes procederem à manutenção das suas redes e dos sistemas de informação a nível interno ou de a externalizarem.

(53) Para evitar impor encargos financeiros e administrativos desproporcionados aos operadores de serviços essenciais e aos prestadores de serviços digitais, os requisitos estabelecidos deverão ser proporcionados em relação ao risco apresentado pelas redes e pelos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. No caso dos prestadores de serviços digitais, esses requisitos não deverão aplicar-se às microempresas nem às pequenas empresas.

(54) As administrações públicas dos Estados-Membros que utilizem serviços oferecidos por prestadores de serviços digitais, em especial serviços de computação em nuvem, poderão exigir que os prestadores desses serviços adotem medidas de segurança adicionais, além das que são normalmente aplicadas pelos prestadores de serviços digitais nos termos dos requisitos previstos na presente diretiva. Deverão poder fazê-lo por meio de obrigações contratuais.

(55) As definições de «mercados em linha», «motores de pesquisa em linha» e «serviços de computação em nuvem» constantes da presente diretiva têm especificamente por objetivo os fins nela previstos, sem prejuízo de quaisquer outros instrumentos.

(56) A presente diretiva não deverá impedir que os Estados-Membros adotem medidas nacionais que exijam que os organismos do setor público garantam requisitos de segurança específicos ao contratarem serviços de computação em nuvem. Essas medidas nacionais deverão aplicar-se ao organismo do setor público em causa, e não ao fornecedor de serviços de computação em nuvem.

(57) Dadas as diferenças fundamentais existentes entre os operadores de serviços essenciais, em especial a sua ligação direta à infraestrutura física, e os prestadores de serviços digitais, nomeadamente a sua natureza transfronteiriça, a presente diretiva deverá seguir uma abordagem diferenciada no que respeita ao nível de harmonização referente a esses dois grupos de entidades. Em relação aos operadores de serviços essenciais, os Estados-Membros deverão ser capazes de identificar os operadores relevantes e de impor requisitos mais rigorosos do que os estabelecidos na presente diretiva. Os Estados-Membros não deverão identificar os prestadores de serviços digitais, uma vez que a presente diretiva se deverá aplicar a todos os prestadores de serviços digitais abrangidos pelo seu âmbito de aplicação. Além disso, a presente diretiva e os atos de execução que dela decorrem deverão garantir aos prestadores de serviços digitais um elevado nível de harmonização no que respeita aos requisitos de segurança e notificação. Isto deverá permitir o tratamento uniforme dos prestadores de serviços digitais em toda a União, de forma proporcional à sua natureza e ao grau de risco com que possam ver-se confrontados.

(58) A presente diretiva não deverá impedir que os Estados-Membros imponham requisitos de segurança e notificação a entidades que não os prestadores de serviços digitais abrangidos pelo seu âmbito de aplicação, sem prejuízo das obrigações que incumbem aos Estados-Membros por força do direito da União.

(59) As autoridades competentes deverão esforçar-se por manter canais informais e de confiança para a partilha de informações. A publicidade dada aos incidentes comunicados às autoridades competentes deverá traduzir o devido equilíbrio entre o interesse do público em ser informado acerca das ameaças e os eventuais danos para os operadores de serviços essenciais e os prestadores de serviços digitais que comunicam esses incidentes ao nível comercial e da sua reputação. Ao cumprirem as obrigações de notificação, as autoridades competentes e as CSIRT deverão prestar especial atenção à necessidade de manter as informações sobre as vulnerabilidades dos produtos estritamente confidenciais até à divulgação das medidas de segurança adequadas para as resolver.

(60) Os prestadores de serviços digitais deverão ser sujeitos a uma supervisão *ex post* ligeira e reativa, justificada pela natureza dos seus serviços e operações. A autoridade competente em causa só deverá, pois, tomar medidas se, por exemplo, o próprio fornecedor de serviços digitais, outra autoridade competente, incluindo uma autoridade competente de outro Estado-Membro, ou um utilizador do serviço lhe provarem que determinado fornecedor de serviços digitais não cumpre os requisitos estabelecidos na presente diretiva, especialmente na sequência da ocorrência de um incidente. A autoridade competente não deverá, pois, ficar sujeita à obrigação geral de supervisionar os prestadores de serviços digitais.

(61) As autoridades competentes deverão dispor dos meios necessários para a execução das suas atribuições, nomeadamente de poderes para obter informações suficientes para avaliar o nível de segurança das redes e dos sistemas de informação.

(62) Os incidentes podem resultar de atividades criminosas para cuja prevenção, investigação e repressão contribuem a coordenação e cooperação estabelecidas entre os operadores de serviços essenciais, os prestadores de serviços digitais, as autoridades competentes e as autoridades responsáveis pela aplicação da lei. Caso se suspeite de que um incidente está relacionado com atividades criminosas graves nos termos do direito da União ou do direito nacional, os Estados-Membros deverão incentivar os operadores de serviços essenciais e os prestadores de serviços digitais a comunicar às autoridades responsáveis pela aplicação da lei os incidentes desse tipo. Em determinados casos, é desejável que o Centro Europeu da Cibercriminalidade (EC3) e a ENISA facilitem a coordenação entre as autoridades competentes e as autoridades responsáveis pela aplicação da lei dos diferentes Estados-Membros.

(63) Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção dos dados deverão cooperar e trocar informações sobre todas as questões pertinentes para combater as eventuais violações de dados pessoais resultantes de incidentes.

(64) No que respeita aos prestadores de serviços digitais, deverá ser atribuída competência ao Estado-Membro no qual o prestador do serviço digital tenha o seu estabelecimento principal na União, o que, em princípio, corresponde ao local onde tem a sua sede. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa organização estável. A forma jurídica de tal organização, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante neste contexto. Este critério não deverá depender do facto

de as redes e os sistemas de informação se situarem fisicamente num determinado local; a presença e a utilização desses sistemas não significam, em si mesmas, que aí se situe o estabelecimento principal e não constituem, pois, critérios aplicáveis à determinação desse estabelecimento.

(65) Os prestadores de serviços digitais não estabelecidos na União que ofereçam serviços na União deverão designar um representante. A fim de determinar se esses prestadores oferecem ou não serviços na União, haverá que apurar se é evidente a sua intenção de oferecer serviços a pessoas num ou mais Estados-Membros. O mero facto de estar acessível na União um sítio *web* do fornecedor de serviços digitais 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 o fornecedor de serviços digitais se encontra estabelecido não é suficiente para determinar essa intenção. Contudo, há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar serviços nessa outra língua, ou a referência a clientes ou utilizadores na União, que podem ser reveladores de que o fornecedor de serviços digitais tenciona oferecer serviços na União. O representante deverá atuar por conta do fornecedor de serviços digitais e deverá poder ser contactado pelas autoridades competentes ou pelas CSIRT. O representante deverá ser explicitamente designado, por mandato escrito do fornecedor de serviços digitais, para atuar por conta deste último relativamente às obrigações que lhe incumbem por força da presente diretiva, incluindo a comunicação de incidentes.

(66) A normalização dos requisitos de segurança é um processo impulsionado pelo mercado. A fim de garantir uma aplicação convergente das normas de segurança, os Estados-Membros deverão incentivar o cumprimento ou a conformidade com normas especificadas a fim de assegurar um elevado nível de segurança das redes e dos sistemas de informação na União. A ENISA deverá prestar assistência aos Estados-Membros, através da prestação de aconselhamento e da formulação de orientações. Para tal, poderá ser útil elaborar normas harmonizadas, nos termos do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([1]).

(67) As entidades que não são abrangidas pelo âmbito de aplicação da presente diretiva podem ser afetadas por incidentes com um impacto importante nos serviços que prestam. Caso essas entidades considerem que é do interesse público notificar a ocorrência de tais incidentes, deverão poder fazê-lo a título voluntário. Tais notificações deverão ser tratadas pela autoridade competente ou pela CSIRT, caso esse tratamento não implique um encargo desproporcionado ou indevido para os Estados-Membros em causa.

(68) A fim de assegurar condições uniformes para a execução da presente diretiva, deverão ser atribuídas competências de execução à Comissão para especificar as disposições processuais necessárias ao funcionamento do grupo de cooperação e os requisitos de segurança e notificação aplicáveis aos prestadores de serviços digitais. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([2]). Quando adotar atos de execução respeitantes às disposições processuais necessárias ao funcionamento do grupo de cooperação, a Comissão deverá ter na melhor conta o parecer da ENISA.

(69) Quando adotar atos de execução respeitantes aos requisitos de segurança aplicáveis aos prestadores de serviços digitais, a Comissão deverá ter na melhor conta o parecer da ENISA e consultar as partes interessadas. Além disso, é incentivada a ter em conta os seguintes exemplos: no que respeita à segurança dos sistemas e das instalações, a segurança física e ambiental, a segurança da prestação de serviços, o controlo do acesso às redes e sistemas de informação e a sua integridade; no que respeita ao tratamento dos incidentes, os procedimentos de tratamento de incidentes, a capacidade de deteção de incidentes e o relato e comunicação de incidentes; no que respeita à gestão da continuidade operacional, a estratégia de continuidade do serviço e os planos de contingência, e as capacidades de recuperação de desastres; e, no que respeita ao acompanhamento, à auditoria e aos testes, as políticas de acompanhamento e registo, os exercícios relativos a planos de contingência, os testes das redes e dos sistemas de informação, as avaliações de segurança e o controlo do cumprimento.

(70) Na aplicação da presente diretiva, a Comissão deverá estabelecer as ligações adequadas com os comités setoriais pertinentes e com os organismos competentes criados a nível da União nos domínios abrangidos pela presente diretiva.

([1]) 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).

([2]) 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).

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

(72) A partilha de informações sobre os riscos e incidentes a nível do grupo de cooperação e da rede de CSIRT e o cumprimento dos requisitos de notificação de incidentes às autoridades nacionais competentes ou às CSIRT poderão requerer o tratamento de dados pessoais. Esse tratamento deverá cumprir o disposto na Diretiva 95/46/CE do Parlamento Europeu e do Conselho ([1]) e no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho ([2]). Na aplicação da presente diretiva deverá respeitar-se, consoante adequado, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ([3]).

(73) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em 14 de junho de 2013 ([4]).

(74) Atendendo a que o objetivo da presente diretiva, a saber, atingir um elevado nível comum de segurança das redes e dos sistemas de informação na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação considerada, ser mais bem alcançado ao 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.

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

ADOTARAM A PRESENTE DIRETIVA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. A presente diretiva estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno.

2. Para o efeito, a presente diretiva:

a) Estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação;

b) Cria um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e de desenvolver a confiança entre eles;

c) Cria uma rede de equipas de resposta a incidentes de segurança informática («rede de CSIRT») a fim de contribuir para o desenvolvimento da confiança entre os Estados-Membros e de promover uma cooperação operacional célere e eficaz;

([1]) Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).
([2]) Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).
([3]) Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).
([4]) JO C 32 de 4.2.2014, p. 19.

d) Estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais;

e) Estabelece a obrigação de os Estados-Membros designarem as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições relacionadas com a segurança das redes e dos sistemas de informação.

3. Os requisitos de segurança e de notificação previstos na presente diretiva não se aplicam às empresas sujeitas aos requisitos previstos nos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE, nem aos prestadores de serviços de confiança sujeitos aos requisitos previstos no artigo 19.º do Regulamento (UE) n.º 910/2014.

4. A presente diretiva é aplicável sem prejuízo da Diretiva 2008/114/CE do Conselho ([1]) e das Diretivas 2011/93/UE ([2]) e 2013/40/UE do Parlamento Europeu e do Conselho ([3]).

5. Sem prejuízo do artigo 346.º do TFUE, as informações que sejam confidenciais nos termos das regras da União e das regras nacionais, tais como as regras de sigilo comercial, só são trocadas com a Comissão e com outras autoridades relevantes nos casos em que esse intercâmbio seja necessário para a aplicação da presente diretiva. As informações trocadas limitam-se ao que for relevante e proporcionado em relação ao objetivo desse intercâmbio. O referido intercâmbio de informações preserva a confidencialidade dessas informações e salvaguarda a segurança e os interesses comerciais dos operadores de serviços essenciais e dos prestadores de serviços digitais.

6. A presente diretiva não prejudica as medidas tomadas pelos Estados-Membros para salvaguardar as funções essenciais do Estado, em especial a fim de salvaguardar a segurança nacional, incluindo medidas de proteção das informações cuja divulgação os Estados-Membros considerem contrária aos interesses essenciais da sua própria segurança, e para manter a ordem pública, em especial a fim de permitir a investigação, a deteção e a repressão de infrações penais.

7. Caso um ato jurídico setorial da União exija que os operadores de serviços essenciais ou os prestadores de serviços digitais garantam a segurança das suas redes e dos seus sistemas de informação ou a notificação de incidentes, são aplicáveis essas disposições desse ato jurídico setorial da União, desde que os seus requisitos tenham pelo menos efeitos equivalentes às obrigações previstas na presente diretiva.

Artigo 2.º

Tratamento de dados pessoais

1. O tratamento de dados pessoais ao abrigo da presente diretiva é efetuado nos termos da Diretiva 95/46/CE.

2. O tratamento de dados pessoais pelas instituições e organismos da União ao abrigo da presente diretiva é efetuado nos termos do Regulamento (CE) n.º 45/2001.

Artigo 3.º

Harmonização mínima

Sem prejuízo do artigo 16.º, n.º 10, e das suas obrigações ao abrigo do direito da União, os Estados-Membros podem adotar ou manter disposições destinadas a atingir um nível mais elevado de segurança das redes e dos sistemas de informação.

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

([2]) 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).

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

Artigo 4.º

Definições

Para efeitos da presente diretiva, entende-se por:

1) «Rede e sistema de informação»,

   a) Uma rede de comunicações eletrónicas na aceção do artigo 2.º, alínea a), da Diretiva 2002/21/CE;

   b) Um dispositivo ou um grupo de dispositivos interligados ou associados, um ou mais dos quais 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 das redes e dos sistemas de informação», a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles;

3) «Estratégia nacional de segurança das redes e dos sistemas de informação», um enquadramento que estabelece objetivos estratégicos e prioridades em matéria de segurança das redes e dos sistemas de informação a nível nacional;

4) «Operador de serviços essenciais», uma entidade pública ou privada pertencente a um dos tipos referidos no anexo II e que cumpre os critérios previstos no artigo 5.º, n.º 2;

5) «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 ([1]), pertencente a um dos tipos enumerados no anexo III;

6) «Prestador de serviços digitais», uma pessoa coletiva que presta um serviço digital;

7) «Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;

8) «Tratamento de incidentes», todos os procedimentos de apoio à deteção, análise e contenção de um incidente, e à resposta ao incidente;

9) «Risco», uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação;

10) «Representante», uma pessoa singular ou coletiva, estabelecida na União, expressamente designada para atuar por conta de um prestador de serviços digitais não estabelecido na União, que pode ser contactada por uma autoridade competente nacional ou por uma CSIRT em vez do prestador de serviços digitais quanto às obrigações que incumbem a este último por força da presente diretiva;

11) «Norma», uma norma na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012;

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

13) «Ponto de troca de tráfego», uma estrutura de rede que permite a interligação de mais de dois sistemas autónomos independentes, 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;

14) «Sistema de nomes de domínio» (DNS), um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio;

([1]) 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).

15) «Prestador de serviços do sistema de nomes de domínio», uma entidade que presta serviços de DNS na Internet;

16) «Registo de nomes de domínio de topo», uma entidade que administra e opera o registo de nomes de domínio da Internet no contexto de um domínio de topo específico;

17) «Mercado em linha», um serviço digital que permite aos consumidores e/ou aos comerciantes, tal como definidos, respetivamente, no artigo 4.º, n.º 1, alínea a) e alínea b), da Diretiva 2013/11/UE do Parlamento Europeu e do Conselho ([1]), celebrarem contratos de venda ou de prestação de serviços por via eletrónica com comerciantes, quer no sítio *web* do mercado em linha, quer no sítio *web* de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha;

18) «Motor de pesquisa em linha», um serviço digital que permite aos utilizadores consultarem, em princípio, todos os sítios *web*, ou sítios *web* numa determinada língua, com base numa pesquisa sobre qualquer assunto, sob a forma de uma palavra-chave, de uma frase ou de outros dados, e que responde fornecendo ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado;

19) «Serviço de computação em nuvem», um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis.

Artigo 5.º

Identificação dos operadores de serviços essenciais

1. Os Estados-Membros identificam, até 9 de novembro de 2018, os operadores de serviços essenciais de cada setor e subsetor referidos no anexo II, estabelecidos no seu território.

2. Os critérios para a identificação dos operadores de serviços essenciais referidos no artigo 4.º, ponto 4, são os seguintes:

a) Uma entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais;

b) A prestação desse serviço depende de redes e sistemas de informação; e

c) Um incidente pode ter efeitos perturbadores importantes na prestação desse serviço.

3. Para efeitos do n.º 1, cada Estado-Membro estabelece uma lista dos serviços a que se refere o n.º 2, alínea a).

4. Para efeitos do n.º 1, caso uma entidade preste um serviço referido no n.º 2, alínea a), em dois ou mais Estados-Membros, estes consultam-se mutuamente. A consulta tem lugar antes de ser tomada uma decisão sobre a identificação.

5. Os Estados-Membros procedem regularmente, e pelo menos de dois em dois anos após 9 de maio de 2018, a uma revisão e, se for caso disso, a uma atualização da lista dos operadores de serviços essenciais identificados.

6. Compete ao grupo de cooperação, de acordo com as atribuições a que se refere o artigo 11.º, apoiar os Estados-Membros na adoção de uma abordagem coerente no processo de identificação dos operadores de serviços essenciais.

7. Para efeitos da avaliação a que se refere o artigo 23.º, os Estados-Membros comunicam à Comissão, até 9 de novembro de 2018 e, posteriormente, de dois em dois anos, as informações necessárias para que esta possa avaliar a aplicação da presente diretiva, em particular a coerência das abordagens dos Estados-Membros relativamente à identificação dos operadores de serviços essenciais. Essas informações incluem, pelo menos, o seguinte:

a) As medidas nacionais que permitem identificar os operadores de serviços essenciais;

([1]) Diretiva 2013/11/UE do Parlamento Europeu e do Conselho, de 21 de maio de 2013, sobre a resolução alternativa de litígios de consumo, que altera o Regulamento (CE) n.º 2006/2004 e a Diretiva 2009/22/CE (Diretiva RAL) (JO L 165 de 18.6.2013, p. 63).

b) A lista dos serviços a que se refere o n.º 3;

c) O número de operadores de serviços essenciais identificados por cada setor referido no anexo II e uma indicação da sua importância dentro do seu setor;

d) Os limiares, caso existam, para determinar o nível de oferta relevante em função do número de utilizadores que dependem desse serviço, tal como referido no artigo 6.º, n.º 1, alínea a), ou da importância desse operador de serviços essenciais em particular, tal como referido no artigo 6.º, n.º 1, alínea f).

A fim de contribuir para a disponibilização de informações comparáveis, a Comissão pode adotar, tendo na melhor conta o parecer da ENISA, orientações técnicas adequadas sobre os parâmetros para as informações referidas no presente número.

Artigo 6.º

Efeito perturbador importante

1. Ao determinar a importância de um efeito perturbador referido no artigo 5.º, n.º 2, alínea c), os Estados-Membros têm em conta, pelo menos, os seguintes fatores transetoriais:

a) O número de utilizadores que dependem dos serviços prestados pela entidade em causa;

b) A dependência de outros setores referidos no anexo II em relação ao serviço prestado por essa entidade;

c) O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais ou a segurança pública;

d) A quota de mercado dessa entidade;

e) A distribuição geográfica, no que se refere à zona que pode ser afetada por um incidente;

f) A importância da entidade para a manutenção de um nível suficiente do serviço, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço.

2. A fim de determinar se um incidente pode ter um efeito perturbador importante, os Estados-Membros têm igualmente em conta, se adequado, fatores setoriais específicos.

CAPÍTULO II

QUADROS NACIONAIS PARA A SEGURANÇA DAS REDES E DOS SISTEMAS DE INFORMAÇÃO

Artigo 7.º

Estratégia nacional de segurança das redes e dos sistemas de informação

1. Cada Estado-Membro adota uma estratégia nacional de segurança das redes e dos sistemas de informação que defina os objetivos estratégicos e as medidas políticas e regulamentares adequadas para alcançar e manter um elevado nível de segurança das redes e dos sistemas de informação e que abrange pelo menos os setores referidos no anexo II e os serviços referidos no anexo III. A estratégia nacional de segurança das redes e dos sistemas de informação contempla, em especial, os seguintes aspetos:

a) Os objetivos e as prioridades da estratégia nacional de segurança das redes e dos sistemas de informação;

b) Um quadro de governação para alcançar os objetivos e as prioridades da estratégia nacional de segurança das redes e dos sistemas de informação, incluindo as funções e responsabilidades dos organismos governamentais e dos outros intervenientes relevantes;

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

d) Uma indicação dos programas de ensino, de sensibilização e de formação relacionados com a estratégia nacional de segurança das redes e dos sistemas de informação;

e) Uma indicação dos planos de investigação e desenvolvimento relacionados com a estratégia nacional de segurança das redes e dos sistemas de informação;

f) Um plano de avaliação dos riscos para identificar riscos;

g) Uma lista dos vários intervenientes envolvidos na execução da estratégia nacional de segurança das redes e dos sistemas de informação.

2. Os Estados-Membros podem solicitar a assistência da ENISA para a elaboração das estratégias nacionais de segurança das redes e dos sistemas de informação.

3. Os Estados-Membros comunicam as suas estratégias nacionais de segurança das redes e dos sistemas de informação à Comissão no prazo de três meses a contar da sua adoção. Ao fazê-lo, os Estados-Membros podem excluir elementos da estratégia relacionados com a segurança nacional.

Artigo 8.º

Autoridades nacionais competentes e pontos de contacto únicos

1. Cada Estado-Membro designa uma ou mais autoridades nacionais competentes em matéria de segurança das redes e dos sistemas de informação («autoridade competente»), que abranjam pelo menos os setores referidos no anexo II e os serviços referidos no anexo III. Os Estados-Membros podem atribuir esse papel a uma ou várias autoridades existentes.

2. As autoridades competentes controlam a aplicação da presente diretiva a nível nacional.

3. Cada Estado-Membro designa um ponto de contacto único nacional para a segurança das redes e dos sistemas de informação («ponto de contacto único»). Os Estados-Membros podem atribuir esse papel a uma autoridade existente. Caso um Estado-Membro designe apenas uma autoridade competente, esta é também o ponto de contacto único.

4. O ponto de contacto único exerce uma função de ligação para assegurar a cooperação transfronteiriça das autoridades dos Estados-Membros com as autoridades competentes de outros Estados-Membros, com o grupo de cooperação a que se refere o artigo 11.º e com a rede de CSIRT a que se refere o artigo 12.º.

5. Os Estados-Membros asseguram que as autoridades competentes e os pontos de contacto únicos disponham de recursos adequados para a executar eficaz e eficientemente as suas atribuições, realizando assim os objetivos da presente diretiva. Os Estados-Membros garantem a cooperação eficaz, eficiente e segura dos representantes designados no grupo de cooperação.

6. Sempre que adequado, e de acordo com o direito nacional, as autoridades competentes e o ponto de contacto único consultam as autoridades nacionais relevantes responsáveis pela aplicação da lei e pela proteção de dados, e cooperam com elas.

7. Cada Estado-Membro notifica sem demora a Comissão da designação da autoridade competente e do ponto de contacto único, das suas atribuições e de quaisquer alterações posteriores das mesmas. Cada Estado-Membro torna pública a sua designação da autoridade competente e do ponto de contacto único. A Comissão publica a lista dos pontos de contacto únicos designados.

Artigo 9.º

Equipas de resposta a incidentes de segurança informática (CSIRT)

1. Cada Estado-Membro designa uma ou mais CSIRT, que cumpram as obrigações estabelecidas no anexo I, ponto1, e que abranjam pelo menos os setores referidos no anexo II e os serviços referidos no anexo III, responsáveis pelo tratamento de riscos e incidentes de acordo com um processo bem definido. As CSIRT podem ser criadas no âmbito de autoridades competentes.

2. Os Estados-Membros asseguram que as CSIRT disponham dos recursos adequados para executar eficazmente as suas atribuições, tal como definidas no anexo I, ponto 2.

Os Estados-Membros garantem a cooperação eficaz, eficiente e segura das suas CSIRT no âmbito da rede de CSIRT a que se refere o artigo 12.º.

3. Os Estados-Membros asseguram que as suas CSIRT tenham acesso a infraestruturas de comunicação e informação adequadas, seguras e resilientes a nível nacional.

4. Os Estados-Membros informam a Comissão sobre o mandato e sobre os principais elementos relativos ao processo de tratamento de incidentes das suas CSIRT.

5. Os Estados-Membros podem solicitar a assistência da ENISA para desenvolver as suas CSIRT.

Artigo 10.º

Cooperação a nível nacional

1. Se forem entidades distintas, a autoridade competente, o ponto de contacto único e a CSIRT do mesmo Estado-Membro cooperam no que diz respeito ao cumprimento das obrigações previstas na presente diretiva.

2. Os Estados-Membros asseguram que as autoridades competentes ou as CSIRT recebam as notificações de incidentes apresentadas nos termos da presente diretiva. Caso um Estado-Membro decida que as CSIRT não devem receber notificações, as CSIRT beneficiam de acesso, na medida do necessário para a execução das suas atribuições, a dados sobre os incidentes notificados por operadores de serviços essenciais, nos termos do artigo 14.º, n.os 3 e 5, ou por prestadores de serviços digitais, nos termos do artigo 16.º, n.os 3 e 6.

3. Os Estados-Membros asseguram que as autoridades competentes ou as CSIRT informem os pontos de contacto únicos sobre as notificações de incidentes apresentadas nos termos da presente diretiva.

Até 9 de agosto de 2018, e, posteriormente, uma vez por ano, o ponto de contacto único apresenta um relatório de síntese ao grupo de cooperação sobre as notificações recebidas, incluindo o número de notificações, a natureza dos incidentes notificados e as medidas tomadas nos termos do artigo 14.º, n.os 3 e 5, e do artigo 16.º, n.os 3 e 6.

CAPÍTULO III

COOPERAÇÃO

Artigo 11.º

Grupo de cooperação

1. É criado um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros, de desenvolver a confiança e de garantir um elevado nível comum de segurança das redes e dos sistemas de informação na União.

O grupo de cooperação executa as suas atribuições com base nos programas de trabalho bienais referidos no n.º 3, segundo parágrafo.

2. O grupo de cooperação é composto por representantes dos Estados-Membros, da Comissão e da ENISA.

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

O secretariado é assegurado pela Comissão.

3. O grupo de cooperação tem as seguintes atribuições:

a) Fornecer orientações estratégicas para as atividades da rede de CSIRT criada nos termos do artigo 12.º;

b) Proceder ao intercâmbio de boas práticas sobre o intercâmbio de informações relativas à notificação de incidentes referida no artigo 14.º, n.ºs 3 e 5, e no artigo 16.º, n.ºs 3 e 6;

c) Proceder ao intercâmbio de boas práticas entre os Estados-Membros e, em colaboração com a ENISA, assistir os Estados-Membros no desenvolvimento de capacidades para garantir a segurança das redes e dos sistemas de informação;

d) Discutir as capacidades e o grau de preparação dos Estados-Membros e, numa base voluntária, avaliar as estratégias nacionais de segurança das redes e dos sistemas de informação e a eficácia das CSIRT, e identificar as boas práticas;

e) Proceder ao intercâmbio de informações e de boas práticas em matéria de sensibilização e formação;

f) Proceder ao intercâmbio de informações e de boas práticas sobre investigação e desenvolvimento em matéria de segurança das redes e dos sistemas de informação;

g) Se for caso disso, proceder ao intercâmbio de experiências em matéria de segurança das redes e dos sistemas de informação com as instituições, os órgãos, os organismos e as agências relevantes da União;

h) Discutir as normas e as especificações referidas no artigo 19.º com os representantes das organizações europeias de normalização relevantes;

i) Recolher informações sobre as boas práticas respeitantes a riscos e incidentes;

j) Analisar anualmente os relatórios de síntese a que se refere o artigo 10.º, n.º 3, segundo parágrafo;

k) Discutir o trabalho realizado no que diz respeito a exercícios de segurança das redes e dos sistemas de informação e a programas de educação e de formação, incluindo o trabalho realizado pela ENISA;

l) Com a assistência da ENISA, proceder ao intercâmbio de boas práticas no que diz respeito à identificação dos operadores de serviços essenciais pelos Estados-Membros, nomeadamente quanto a dependências transfronteiriças, referentes a riscos e incidentes;

m) Discutir as formas de comunicação das notificações de incidentes referidas nos artigos 14.º e 16.º.

Até 9 de fevereiro de 2018, e, posteriormente, de dois em dois anos, o grupo de cooperação define um programa de trabalho relativo às ações a empreender para cumprir os seus objetivos e as suas atribuições, que deve ser coerente com os objetivos da presente diretiva.

4. Para efeitos da avaliação a que se refere o artigo 23.º, o grupo de cooperação elabora, até 9 de agosto de 2018, e, posteriormente, de 18 em 18 meses, um relatório de avaliação da experiência adquirida com a cooperação estratégica realizada ao abrigo do presente artigo.

5. A Comissão adota atos de execução que estabeleçam as disposições processuais necessárias para o funcionamento do grupo de cooperação. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 22.º, n.º 2.

Para efeitos de aplicação do primeiro parágrafo, a Comissão apresenta o primeiro projeto de ato de execução ao Comité a que se refere o artigo 22.º, n.º 1, até 9 de fevereiro de 2017.

Artigo 12.º

Rede de CSIRT

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

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

3. A rede de CSIRT tem as seguintes atribuições:

a) Proceder ao intercâmbio de informações sobre os serviços, as operações e a capacidade de cooperação das CSIRT;

b) A pedido de um representante de uma CSIRT de um Estado-Membro potencialmente afetado por um incidente, proceder ao intercâmbio e à discussão de informações não comercialmente sensíveis relacionadas com esse incidente e com riscos conexos; contudo, uma CSIRT de um Estado-Membro pode recusar-se a contribuir para essa discussão se existir o risco de a investigação do incidente ser prejudicada;

c) Proceder ao intercâmbio e facultar informações não confidenciais, numa base voluntária, sobre incidentes específicos;

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

e) Prestar apoio aos Estados-Membros na reação a incidentes transfronteiriços com base na sua assistência mútua voluntária;

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

   i) às categorias de riscos e de incidentes,

   ii) aos alertas rápidos,

   iii) à assistência mútua,

   iv) aos princípios e às formas de coordenação na resposta dos Estados-Membros a riscos e incidentes de dimensão transfronteiriça;

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

h) Discutir os ensinamentos retirados dos exercícios de segurança das redes e dos sistemas de informação, incluindo os exercícios organizados pela ENISA;

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

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

4. Para efeitos da avaliação a que se refere o artigo 23.º, a rede de CSIRT elabora, até 9 de agosto de 2018, e, posteriormente, de 18 em 18 meses, um relatório de avaliação da experiência adquirida com a cooperação operacional ao abrigo do presente artigo, incluindo conclusões e recomendações. Esse relatório é apresentado também ao grupo de cooperação.

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

Artigo 13.º

Cooperação internacional

A União pode celebrar acordos internacionais, nos termos do artigo 218.º do TFUE, com países terceiros ou organizações internacionais que permitam e organizem a participação destes últimos em algumas atividades do grupo de cooperação. Esses acordos têm em conta a necessidade de garantir uma proteção de dados adequada.

CAPÍTULO IV

SEGURANÇA DAS REDES E DOS SISTEMAS DE INFORMAÇÃO DOS OPERADORES DE SERVIÇOS ESSENCIAIS

Artigo 14.º

Requisitos de segurança e notificação de incidentes

1. Os Estados-Membros asseguram que os operadores de serviços essenciais tomem as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

2. Os Estados-Membros asseguram que os operadores de serviços essenciais tomem as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.

3. Os Estados-Membros asseguram que os operadores de serviços essenciais notifiquem as autoridades competentes ou as CSIRT, sem demora injustificada, dos incidentes com um impacto importante na continuidade dos serviços essenciais por si prestados. As notificações incluem informações que permitam às autoridades competentes ou às CSIRT determinar o impacto transfronteiriço dos incidentes. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar a importância do impacto de um incidente são tidos em conta, em especial, os seguintes parâmetros:

a) O número de utilizadores afetados pela perturbação do serviço essencial;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente.

5. Com base nas informações prestadas na notificação pelo operador de serviços essenciais, a autoridade competente ou a CSIRT informam os outros Estados-Membros afetados caso o incidente tenha um impacto importante na continuidade dos serviços essenciais nesses Estados-Membros. Ao fazê-lo, a autoridade competente ou a CSIRT salvaguardam, de acordo com o direito da União ou com a legislação nacional conforme com o direito da União, a segurança e os interesses comerciais do operador de serviços essenciais, bem como a confidencialidade das informações prestadas na sua notificação.

Sempre que as circunstâncias o permitam, a autoridade competente ou a CSIRT prestam ao operador de serviços essenciais notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente.

A pedido da autoridade competente ou da CSIRT, o ponto de contacto único transmite as notificações referidas no primeiro parágrafo aos pontos de contacto únicos dos outros Estados-Membros afetados.

6. Após consultar o operador de serviços essenciais notificante, a autoridade competente ou a CSIRT podem informar o público sobre incidentes específicos, caso seja necessário sensibilizá-lo para evitar um incidente ou para tratar um incidente em curso.

7. As autoridades competentes podem elaborar e adotar, agindo em conjunto no âmbito do grupo de cooperação, orientações sobre as circunstâncias em que os operadores de serviços essenciais são obrigados a notificar incidentes, inclusive sobre os parâmetros para determinar a importância do impacto de um incidente, tal como referido no n.º 4.

Artigo 15.º

Aplicação e execução

1. Os Estados-Membros asseguram que as autoridades competentes disponham dos poderes e dos meios necessários para avaliar o cumprimento das obrigações que incumbem aos operadores de serviços essenciais por força do artigo 14.º, bem como os seus efeitos na segurança das redes e dos sistemas de informação.

2. Os Estados-Membros asseguram que as autoridades competentes disponham de poderes e meios para exigir que os operadores de serviços essenciais forneçam:

a) As informações necessárias para avaliar a segurança das suas redes e sistemas de informação, incluindo a documentação relativa às suas políticas de segurança;

b) Provas da aplicação efetiva das políticas de segurança, tais como os resultados de uma auditoria de segurança efetuada pela autoridade competente ou por um auditor qualificado e que, no último caso, facultem os resultados dessa auditoria, incluindo os elementos de prova subjacentes, à autoridade competente.

Ao requererem essas informações ou essas provas, as autoridades competentes declaram a finalidade do seu pedido e especificam as informações requeridas.

3. Na sequência da avaliação das informações ou dos resultados das auditorias de segurança a que se refere o n.º 2, as autoridades competentes podem emitir instruções vinculativas dirigidas aos operadores de serviços essenciais, para que estes corrijam as deficiências detetadas.

4. Quando tratarem de incidentes que tenham dado origem à violação de dados pessoais, as autoridades competentes trabalham em estreita colaboração com as autoridades encarregadas da proteção de dados.

CAPÍTULO V

SEGURANÇA DAS REDES E DOS SISTEMAS DE INFORMAÇÃO DOS PRESTADORES DE SERVIÇOS DIGITAIS

Artigo 16.º

Requisitos de segurança e notificação de incidentes

1. Os Estados-Membros asseguram que os prestadores de serviços digitais identifiquem e tomem as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços referidos no anexo III na União. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, e devem ter em conta:

a) A segurança dos sistemas e das instalações;

b) O tratamento dos incidentes;

c) A gestão da continuidade das atividades;

d) O acompanhamento, a auditoria e os testes realizados;

e) A conformidade com as normas internacionais.

2. Os Estados-Membros asseguram que os prestadores de serviços digitais tomem medidas para evitar os incidentes que afetem a segurança das suas redes e sistemas de informação e para reduzir ao mínimo o seu impacto no que diz respeito aos serviços referidos no anexo III oferecidos na União, a fim de assegurar a continuidade desses serviços.

3. Os Estados-Membros asseguram que os prestadores de serviços digitais notifiquem a autoridade competente ou a CSIRT, sem demora injustificada, dos incidentes com impacto substancial na prestação dos serviços referidos no anexo III por si oferecidos na União. As notificações incluem informações que permitam à autoridade competente ou à CSIRT determinar a importância dos impactos transfronteiriços. A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4. A fim de determinar se o impacto de um incidente é substancial, são tidos em conta, em especial, os seguintes parâmetros:

a) O número de utilizadores afetados pelo incidente, nomeadamente de utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente;

d) O nível de gravidade da perturbação do funcionamento do serviço;

e) A extensão do impacto nas atividades económicas e societais.

A obrigação de notificar um incidente só se aplica se o prestador de serviços digitais tiver acesso às informações necessárias para avaliar o impacto de um incidente em função dos parâmetros a que se refere o primeiro parágrafo.

5. Se um operador de serviços essenciais depender de um terceiro prestador de serviços digitais para a prestação de um serviço essencial para a manutenção de atividades societais e económicas cruciais, notifica todos os impactos importantes na continuidade dos seus serviços, decorrentes dos incidentes que afetem o prestador de serviços digitais.

6. Se adequado, e em particular se os incidentes referidos no n.º 3 disserem respeito a dois ou mais Estados-Membros, as autoridades competentes ou as CSIRT informam os outros Estados-Membros afetados. Ao fazê-lo, as autoridades competentes, as CSIRT e os pontos de contacto únicos salvaguardam, de acordo com o direito da União ou com a legislação nacional conforme com o direito da União, a segurança e os interesses comerciais do prestador de serviços digitais, bem como a confidencialidade das informações prestadas.

7. Após consultar o prestador de serviços digitais em causa, a autoridade competente ou a CSIRT e, se for caso disso, as autoridades ou as CSIRT de outros Estados-Membros em causa, podem informar o público sobre incidentes específicos ou exigir que o prestador de serviços digitais o faça, caso seja necessário sensibilizar o público para evitar um incidente ou para tratar um incidente em curso, ou caso a divulgação do incidente seja de interesse público.

8. A Comissão adota atos de execução que especifiquem mais pormenorizadamente os elementos referidos no n.º 1 e os parâmetros enumerados no n.º 4 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 22.º, n.º 2, até 9 de agosto de 2017.

9. A Comissão pode adotar atos de execução que definam os formatos e os procedimentos aplicáveis aos requisitos de notificação. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 22.º, n.º 2.

10. Sem prejuízo do artigo 1.º, n.º 6, os Estados-Membros não impõem aos prestadores de serviços digitais requisitos adicionais em matéria de segurança ou de notificação.

11. O capítulo V não se aplica às microempresas nem às pequenas empresas, tal como definidas na Recomendação 2003/361/CE da Comissão ([1]).

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

Artigo 17.º

Aplicação e execução

1. Os Estados-Membros asseguram que as autoridades competentes tomem medidas, se necessário, de supervisão *ex post*, caso lhes tenham sido apresentadas provas de que um prestador de serviços digitais não cumpre os requisitos estabelecidos no artigo 16.º. As provas podem ser apresentadas por uma autoridade competente de outro Estado-Membro em que o serviço seja prestado.

2. Para efeitos do n.º 1, as autoridades competentes dispõem dos poderes e dos meios necessários para exigir que os prestadores de serviços digitais:

a) Lhes forneçam as informações necessárias para avaliar a segurança das suas redes e sistemas de informação, incluindo a documentação relativa às suas políticas de segurança;

b) Corrijam qualquer incumprimento dos requisitos previstos no artigo 16.º.

3. Se um prestador de serviços digitais tiver o seu estabelecimento principal ou estiver representado num Estado-Membro, mas as suas redes e os seus sistemas de informação estiverem situados noutro ou noutros Estados-Membros, a autoridade competente do Estado-Membro do estabelecimento principal ou do representante e as autoridades competentes dos outros Estados-Membros cooperam entre si e prestam assistência mútua, na medida do necessário. Essa assistência e cooperação podem abranger o intercâmbio de informações entre as autoridades competentes em causa e os pedidos para que as medidas de supervisão a que se refere o n.º 2 sejam tomadas.

Artigo 18.º

Competência e territorialidade

1. Para efeitos da presente diretiva, considera-se que um prestador de serviços digitais está sob a jurisdição do Estado-Membro no qual tem o seu estabelecimento principal. Considera-se que um prestador de serviços digitais tem o seu estabelecimento principal num Estado-Membro quando tiver a sua sede nesse Estado-Membro.

2. Um prestador de serviços digitais que não esteja estabelecido na União, mas que ofereça os serviços referidos no anexo III na da União, designa um representante na União. O representante fica estabelecido num dos Estados-Membros em que os serviços são oferecidos. Considera-se que o prestador de serviços digitais está sob a jurisdição do Estado-Membro em que o representante está estabelecido.

3. A designação de um representante pelo prestador de serviços digitais não prejudica as ações judiciais que possam ser intentadas contra o próprio prestador de serviços digitais.

CAPÍTULO VI

NORMALIZAÇÃO E NOTIFICAÇÃO VOLUNTÁRIA

Artigo 19.º

Normalização

1. A fim de promover a aplicação convergente do artigo 14.º, n.ºs 1 e 2, e do artigo 16.º, n.ºs 1 e 2, os Estados-Membros incentivam, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, a utilização de normas e especificações europeias ou internacionalmente aceites plicáveis à segurança das redes e dos sistemas de informação.

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

Artigo 20.º

Notificação voluntária

1. Sem prejuízo do artigo 3.º, as entidades que não tenham sido identificadas como operadores de serviços essenciais e que não sejam prestadores de serviços digitais podem notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados.

2. No tratamento das notificações, os Estados-Membros aplicam o procedimento previsto no artigo 14.º. Os Estados-Membros podem dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias. As notificações voluntárias só são tratadas se esse tratamento não constituir um ónus desproporcionado ou indevido para os Estados-Membros em causa.

A notificação voluntária não pode dar origem à imposição à entidade notificadora de obrigações às quais esta não teria sido sujeita se não tivesse procedido a essa notificação.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Artigo 21.º

Sanções

Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação do disposto nas 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 dessas regras e dessas medidas até 9 de maio de 2018, e também, imediatamente, de qualquer alteração ulterior das mesmas.

Artigo 22.º

Procedimento de comité

1. A Comissão é assistida pelo Comité de Segurança das Redes e dos Sistemas de Informação. 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.

Artigo 23.º

Avaliação

1. A Comissão apresenta um relatório ao Parlamento Europeu e ao Conselho, até 9 de maio de 2019, que avalie a coerência da abordagem adotada pelos Estados-Membros na identificação dos operadores de serviços essenciais.

2. A Comissão avalia periodicamente a aplicação da presente diretiva e apresenta um relatório ao Parlamento Europeu e ao Conselho. 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. Na sua avaliação, a Comissão avalia igualmente as listas constantes dos anexos II e III e a coerência na identificação dos operadores de serviços essenciais e de serviços nos setores referidos no anexo II. O primeiro relatório é apresentado até 9 de maio de 2021.

Artigo 24.º

Medidas transitórias

1. Sem prejuízo do artigo 25.º, e a fim de proporcionar aos Estados-Membros possibilidades adicionais para cooperarem de forma adequada durante o período de transposição, o grupo de cooperação e a rede de CSIRT começam a desempenhar as suas funções, definidas respetivamente nos artigos 11.º, n.º 3, e 12.º, n.º 3, até 9 de fevereiro de 2017.

2. No período compreendido entre 9 de fevereiro de 2017 e 9 de novembro de 2018, e a fim de apoiar os Estados-Membros na adoção de uma abordagem coerente no processo de identificação dos operadores de serviços essenciais, o grupo de cooperação discute o processo, o conteúdo e o tipo de medidas nacionais que permitam identificar os operadores de serviços essenciais num setor específico, de acordo com os critérios enunciados nos artigos 5.º e 6.º. O grupo de cooperação discute também, a pedido de um Estado-Membro, projetos específicos de medidas nacionais desse Estado-Membro que permitam identificar operadores de serviços essenciais num setor específico, de acordo com os critérios enunciados nos artigos 5.º e 6.º.

3. Até 9 de fevereiro de 2017, e para efeitos do presente artigo, os Estados-Membros asseguram uma representação adequada no grupo de cooperação e na rede de CSIRT.

Artigo 25.º

Transposição

1. Os Estados-Membros adotam e publicam, até 9 de maio de 2018, as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Do facto informam imediatamente a Comissão.

Os Estados-Membros aplicam essas disposições a partir de 10 de maio de 2018.

Quando os Estados-Membros adotarem essas disposições, estas incluem uma remissão para a presente diretiva ou são acompanhadas dessa remissão aquando da sua publicação oficial. Os Estados-Membros estabelecem o modo como deve ser feita a remissão.

2. Os Estados-Membros comunicam à Comissão o texto das principais disposições de direito interno que adotarem no domínio regulado pela presente diretiva.

Artigo 26.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 27.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Estrasburgo, em 6 de julho de 2016.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
M. SCHULZ	I. KORČOK

ANEXO I

OBRIGAÇÕES E ATRIBUIÇÕES DAS EQUIPAS DE RESPOSTA A INCIDENTES DE SEGURANÇA INFORMÁTICA (CSIRT)

As obrigações e as atribuições das CSIRT devem ser definidas de modo adequado e claro, com base nas políticas e/ou na regulamentação nacionais. Devem incluir o seguinte:

1. Obrigações das CSIRT

   a) As CSIRT devem garantir uma ampla disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais, e devem dispor de vários meios para contactar outras CSIRT e para ser contactadas a qualquer momento. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos da sua base de clientes e dos parceiros de cooperação;

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

   c) Continuidade operacional:

      i) as CSIRT devem estar equipadas com um sistema adequado de gestão e encaminhamento dos pedidos, a fim de facilitar as transferências,

      ii) as CSIRT devem dispor de pessoal suficiente capaz de assegurar a sua disponibilidade a qualquer momento,

      iii) as CSIRT devem apoiar-se numa infraestrutura cuja continuidade seja assegurada; para esse efeito, devem dispor de sistemas redundantes e de espaço de trabalho alternativos;

   d) As CSIRT devem poder participar, se assim o entenderem, em redes de cooperação internacional.

2. Atribuições das CSIRT

   a) As atribuições das CSIRT devem incluir pelo menos o seguinte:

      i) monitorizar os incidentes a nível nacional,

      ii) ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às partes interessadas relevantes sobre riscos e incidentes,

      iii) intervir em caso de incidentes,

      iv) proceder à análise dinâmica dos riscos e dos incidentes e ter uma visão geral da situação,

      v) participar na rede de CSIRT;

   b) As CSIRT devem estabelecer relações de cooperação com o setor privado;

   c) A fim de facilitar a cooperação, as CSIRT devem promover a adoção e a utilização de práticas comuns ou normalizadas para:

      i) os procedimentos de gestão de risco e de incidentes,

      ii) os sistemas de classificação de incidentes, de risco e de informações.

ANEXO II

TIPOS DE ENTIDADES PARA EFEITOS DO ARTIGO 4.º, PONTO 4

Setores	Subsetores	Tipo de entidades
1. Energia	a) Eletricidade	— Empresa de eletricidade na aceção do artigo 2.º, ponto 35, da Diretiva 2009/72/CE do Parlamento Europeu e do Conselho ([1]), que exerce a atividade de «comercialização» na aceção do artigo 2.º, ponto 19, dessa diretiva
		— Operadores da rede de distribuição na aceção do artigo 2.º, ponto 6, da Diretiva 2009/72/CE
		— Operadores da rede de transporte na aceção do artigo 2.º, ponto 4, da Diretiva 2009/72/CE
	b) Petróleo	— Operadores de oleodutos de petróleo
		— Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
	c) Gás	— Empresas de comercialização na aceção do artigo 2.º, ponto 8, da Diretiva 2009/73/CE do Parlamento Europeu e do Conselho ([2])
		— 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
2. Transportes	a) Transporte aéreo	— Transportadoras aéreas na aceção do artigo 3.º, ponto 4, do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho ([3])
		— Entidades gestoras aeroportuárias na aceção do artigo 2.º, ponto 2, da Diretiva 2009/12/CE do Parlamento Europeu e do Conselho ([4]), aeroportos na aceção do artigo 2.º, ponto 1, dessa diretiva, incluindo os aeroportos principais constantes da lista do anexo II, secção 2, do Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho ([5]), e as entidades que exploram instalações anexas existentes dentro dos aeroportos

Setores	Subsetores	Tipo de entidades
		— 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 ([6])
	b) Transporte ferroviário	— Gestores de infraestruturas na aceção do artigo 3.º, ponto 2, da Diretiva 2012/34/UE do Parlamento Europeu e do Conselho ([7])
		— Empresas ferroviárias na aceção do artigo 3.º, ponto 1, da Diretiva 2012/34/UE, incluindo os operadores de instalações de serviço na aceção do artigo 3.º, ponto 12, da Diretiva 2012/34/UE
	c) Transporte marítimo e por vias navegáveis interiores	— 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 ([8]), 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 ([9]), 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 na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho ([10])
	d) Transporte rodoviário	— Autoridades rodoviárias na aceção do artigo 2.º, ponto 12, do Regulamento Delegado (UE) n.º 2015/962 da Comissão ([11]), responsáveis pelo controlo da gestão do tráfego
		— 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 ([12])
3. Setor bancário		Instituições de crédito na aceção do artigo 4.º, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho ([13])
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 ([14])
		— Contrapartes centrais na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho ([15])
5. Setor da saúde	Instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas)	Prestadores de cuidados de saúde na aceção do artigo 3.º, alínea g), da Diretiva 2011/24/UE do Parlamento Europeu e do Conselho ([16])

Setores	Subsetores	Tipo de entidades
6. Forne cimento e distribuição de água potável		Fornecedores e distribuidores de água destinada ao consumo humano, na aceção do artigo 2.º, ponto 1, alínea a), da Diretiva 98/83/CE do Conselho ([17]), mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais
7. Infraestruturas digitais		— Pontos de troca de tráfego
		— Prestadores de serviços de DNS
		— Registos de nomes de domínio de topo

([1]) Diretiva 2009/72/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece regras comuns para o mercado interno da eletricidade e que revoga a Diretiva 2003/54/CE (JO L 211 de 14.8.2009, p. 55).
([2]) 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).
([3]) 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).
([4]) Diretiva 2009/12/CE do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativa às taxas aeroportuárias (JO L 70 de 14.3.2009, p. 11).
([5]) Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2013, relativo às orientações da União para o desenvolvimento da rede transeuropeia de transportes e que revoga a Decisão n.º 661/2010/UE (JO L 348 de 20.12.2013, p. 1).
([6]) Regulamento (CE) n.º 549/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que estabelece o quadro para a realização do céu único europeu («regulamento-quadro») (JO L 96 de 31.3.2004, p. 1).
([7]) Diretiva 2012/34/UE do Parlamento Europeu e do Conselho, de 21 de novembro de 2012, que estabelece um espaço ferroviário europeu único (JO L 343 de 14.12.2012, p. 32).
([8]) Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, de 31 de março de 2004, relativo ao reforço da proteção dos navios e das instalações portuárias (JO L 129 de 29.4.2004, p. 6).
([9]) Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, de 26 de outubro de 2005, relativa ao reforço da segurança nos portos (JO L 310 de 25.11.2005, p. 28).
([10]) Diretiva 2002/59/CE do Parlamento Europeu e do Conselho, de 27 de junho de 2002, relativa à instituição de um sistema comunitário de acompanhamento e de informação do tráfego de navios e que revoga a Diretiva 93/75/CEE do Conselho (JO L 208 de 5.8.2002, p. 10).
([11]) 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).
([12]) 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).
([13]) Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).
([14]) 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).
([15]) Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 201 de 27.7.2012, p. 1).
([16]) 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).
([17]) Diretiva 98/83/CE do Conselho, de 3 de novembro de 1998, relativa à qualidade da água destinada ao consumo humano (JO L 330 de 5.12.1998, p. 32).

ANEXO III

TIPOS DE SERVIÇOS DIGITAIS PARA EFEITOS DO ARTIGO 4.º, PONTO 5

1. Mercados em linha.
2. Motores de pesquisa em linha.
3. Serviços de computação em nuvem.