COMISSÃO
EUROPEIA

Bruxelas, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ANEXO

da

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Tirar o maior partido da SIR – Para uma execução efetiva da Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

ÍNDICE:

ANEXO

1. Introdução.

O presente anexo visa contribuir para uma aplicação, transposição e execução eficaz da Diretiva (UE) 2016/1148, relativa à segurança das redes e da informação em toda a União[1] (a seguir designada «Diretiva SRI» ou a «diretiva») e a ajudar os Estados-Membros a garantir que a legislação da UE é aplicada de forma eficaz. Mais concretamente, os seus objetivos específicos consistem em três vertentes: a) proporcionar às autoridades nacionais uma visão mais clara sobre as obrigações constantes da Diretiva que lhes são aplicáveis; b) garantir a execução eficaz das disposições da Diretiva aplicáveis às entidades sujeitas a obrigações em matéria de requisitos de segurança e de notificação de incidentes; c) contribuir globalmente para garantir segurança jurídica a todos os intervenientes pertinentes.

Para o efeito, o presente anexo fornece orientações sobre os seguintes aspetos, que são essenciais para a consecução do objetivo global do Diretiva SRI, ou seja, garantir um elevado nível comum de segurança das redes e sistemas de informação na UE, nos quais assenta o funcionamento da nossa sociedade e da nossa economia:

- A obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação (ponto 2);
- A criação de autoridades nacionais competentes, pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (ponto 3);
- Os requisitos de segurança e de notificação de incidentes aplicáveis aos operadores de serviços essenciais e aos prestadores de serviços digitais (ponto 4); e
- A relação entre a Diretiva SRI e outra legislação (ponto 5).

Para elaborar as presentes orientações, a Comissão utilizou dados e análises recolhidos durante a fase de preparação da diretiva, o contributo da Agência da União Europeia para a Segurança das Redes e da Informação («ENISA») e do grupo de cooperação. Recorreu também às experiências de determinados Estados-Membros. Quando adequado, a Comissão tomou em consideração os princípios orientadores para a interpretação do direito da UE: a redação, o contexto e os objetivos da Diretiva SRI. Atendendo a que a transposição da diretiva não foi concluída, ainda não foi proferida qualquer decisão do Tribunal de Justiça da União Europeia (TJUE) nem dos tribunais nacionais. Por conseguinte, não é possível recorrer à jurisprudência, para efeitos de orientação.

A compilação destas informações num documento único pode permitir aos Estados-Membros obterem uma visão geral adequada da diretiva e ter esta informação em conta durante a elaboração das respetivas legislações nacionais. Ao mesmo tempo, a Comissão sublinha que o

[1] 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. A diretiva entrou em vigor em 8 de agosto de 2016.

presente anexo não é vinculativo, nem pretende criar novas regras. A última palavra na interpretação do direito da UE cabe ao Tribunal de Justiça (TJUE).

2. Estratégia nacional de segurança das redes e dos sistemas de informação

Nos termos do artigo 7.º da Diretiva SRI, cada Estado-Membro deve adotar uma estratégia nacional de segurança das redes e dos sistemas de informação que pode ser considerada sinónimo da expressão «estratégia nacional de cibersegurança» («ENC»). A função de uma estratégia nacional consiste em definir os objetivos estratégicos e as medidas políticas e regulamentares adequadas em matéria de cibersegurança. O conceito de ENC é amplamente utilizado na Europa e a nível internacional, nomeadamente no contexto das atividades da ENISA com os Estados-Membros sobre as estratégias nacionais que recentemente deram origem a uma versão atualizada do guia de boas práticas sobre a ENC[2].

No presente ponto, a Comissão especifica como a Diretiva SRI reforça o grau de preparação dos Estados-Membros ao exigir que estes disponham de estratégias nacionais sólidas em matéria de segurança das redes e dos sistemas de informação (artigo 7.º). Para tal, são abordados os seguintes aspetos: a) o âmbito de aplicação da estratégia; b) o conteúdo e o procedimento para a adoção da mesma.

Como adiante descrito de forma mais pormenorizada, a correta transposição do artigo 7.º da Diretiva SRI é fundamental para a concretização dos objetivos da diretiva e exige a afetação de recursos financeiros e humanos adequados para o efeito.

2.1. Âmbito de aplicação da estratégia nacional.

Em conformidade com a redação do artigo 7.º, a obrigação de adotar uma ENC aplica-se apenas aos setores referidos no anexo II (ou seja, energia, transportes, banca, mercados financeiros, saúde, abastecimento e distribuição de água potável e infraestruturas digitais) e aos serviços referidos no anexo III (mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem) da diretiva.

O artigo 3.º da diretiva enuncia especificamente o princípio da harmonização mínima, nos termos do qual os Estados-Membros podem adotar ou manter disposições destinadas a atingir um nível mais elevado de segurança das redes e dos sistemas de informação. A aplicação deste princípio à obrigação de adotar uma «ENC» permite aos Estados-Membros incluir mais setores e serviços do que os abrangidos pelo anexo II e III da Diretiva.

No entender da Comissão, e à luz do objetivo da Diretiva SRI, ou seja, alcançar um elevado nível comum de segurança das redes e sistemas de informação na União[3], seria aconselhável desenvolver uma estratégia nacional que contemplasse todos os aspetos relevantes da sociedade e da economia, e não apenas os setores e os serviços digitais abrangidos,

[2] ENISA, *National Cyber-Security Strategy Good Practice* 2016. Disponível em: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Ver o artigo 1.º, n.º 1.

respetivamente, nos anexos II e III da Diretiva SRI Tal está em consonância com as melhores práticas internacionais [ver as orientações da União Internacional das Telecomunicações (UIT) e a análise da OCDE referidas mais adiante] e a Diretiva SRI.

Tal como mais adiante se explica, isto é sobretudo válido em relação às administrações públicas responsáveis por setores e serviços que não os enumerados nos anexos II e III da Diretiva. As administrações públicas podem tratar informações sensíveis, que justificam a necessidade de serem abrangidas por uma ENC e por planos de gestão que evitem fugas e garantam a proteção adequada dessa informação.

2.2. Conteúdo e procedimento para a adoção das estratégias nacionais.

Nos termos do artigo 7.º da Diretiva SRI, uma ENC deve incluir, pelo menos, os seguintes elementos:

i) os objetivos e as prioridades da estratégia nacional de segurança das redes e dos sistemas de informação,
ii) um quadro de governação para alcançar os objetivos e as prioridades da estratégia nacional,
iii) a identificação das medidas de preparação, de resposta e de recuperação, incluindo a cooperação entre os setores público e privado,
iv) uma indicação dos programas de ensino, de sensibilização e de formação pertinentes,
v) uma indicação dos planos de investigação e desenvolvimento,
vi) um plano de avaliação dos riscos para identificar riscos,
vii) uma lista dos vários intervenientes envolvidos na execução da estratégia.

Nem o artigo 7.º, nem o considerando 29, que lhe corresponde, especificam os requisitos necessários para a adoção de uma ENC ou fornecem informações mais pormenorizadas sobre o conteúdo da ENC. No que diz respeito ao processo e aos elementos adicionais relacionados com o conteúdo da ENC, a Comissão considera a abordagem a seguir apresentada como uma forma adequada de adotar uma ENC. Esta baseia-se na análise das experiências de Estados-Membros e de países terceiros no desenvolvimento das suas próprias estratégias. Outra fonte de informação é a ferramenta de formação da ENISA em matéria de ENC, disponível no sítio da agência sob a forma de vídeos e suportes multimédia descarregáveis[4].

2.3. Processo e questões a abordar.

O processo de elaboração e de posterior adoção de uma estratégia nacional é complexo e diversificado, exigindo um envolvimento constante com peritos em matéria de cibersegurança, a sociedade civil e o sistema político nacional, caso se pretenda que seja eficaz e bem-sucedido. Uma condição *sine qua non* é o apoio administrativo superior, pelo menos ao nível de uma secretaria de Estado, ou equivalente, do ministério responsável, bem como o patrocínio político. A fim de concluir com êxito uma ENC, pode considerar-se o seguinte processo de cinco etapas (ver figura 1):

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool.

Primeira etapa — **Estabelecimento de princípios orientadores e objetivos estratégicos decorrentes da estratégia.**

Em primeiro lugar, as autoridades nacionais competentes devem definir alguns elementos fundamentais a incluir na ENC, nomeadamente saber quais são os resultados pretendidos, ou os «*objetivos e prioridades*», na redação da Diretiva (artigo 7.º, n.º 1, alínea a)), de que modo tais resultados complementam as políticas económicas e sociais nacionais e são compatíveis com as prerrogativas e as obrigações decorrentes do estatuto de Estado-Membro da União Europeia. Os objetivos devem ser específicos, mensuráveis, realizáveis, realistas e limitados no tempo (SMART). Um exemplo ilustrativo é o seguinte: «*Garantimos que esta estratégia [calendarizada] assenta num conjunto de parâmetros rigorosos e abrangentes de acordo com os quais medimos os progressos realizados no sentido dos resultados que precisamos de alcançar*»[5]

O que precede inclui também uma avaliação política no sentido de determinar se é possível obter um orçamento significativo para disponibilizar recursos destinados à execução da estratégia. Apresenta igualmente uma descrição do âmbito de aplicação pretendido para a estratégia e das diferentes categorias de partes interessadas dos setores público e privado que devem participar na elaboração dos vários objetivos e medidas.

Esta primeira etapa poderá ser alcançada mediante seminários específicos com altos funcionários dos ministérios e políticos, moderados por especialistas em cibersegurança dotados de elevadas competências comunicacionais e que consigam destacar as implicações da escassez ou inexistência de cibersegurança para uma economia e sociedade digital moderna.

Segunda etapa — **Desenvolvimento do conteúdo da estratégia.**

A estratégia deverá incluir medidas de capacitação, ações calendarizadas e indicadores-chave de desempenho para a consequente avaliação, aperfeiçoamento e melhoria, após um determinado período de execução. Estas medidas devem apoiar os objetivos, as prioridades e os resultados estabelecidos como princípios orientadores. A necessidade de incluir medidas de capacitação é estipulada no artigo 7.º, n.º 1, alínea c), da Diretiva SRI.

Recomenda-se que seja constituído um grupo diretor, presidido pelo ministério responsável, para gerir o processo de elaboração e facilitar a disponibilização de contributos. Este objetivo poderá ser alcançado por meio de um conjunto de grupos de redação constituídos por funcionários e peritos competentes dedicados a temas genéricos fundamentais, por exemplo, a avaliação de riscos, o planeamento de contingência, a gestão de incidentes, o desenvolvimento de competências, a sensibilização, a investigação e desenvolvimento industrial, etc. Cada setor (por exemplo, energia, transportes, etc.) será também convidado separadamente a avaliar as implicações da sua inclusão, nomeadamente a disponibilização de recursos, e envolver-se-ão os operadores de serviços essenciais e os principais prestadores de serviços digitais designados para que ajudem a definir prioridades e apresentem propostas para o processo de

[5] Excerto da estratégia nacional de cibersegurança do Reino Unido, 2016-2021, página 67.

elaboração. A participação de partes interessadas a nível setorial é também essencial, tendo em conta a necessidade de assegurar uma aplicação harmonizada da diretiva entre os diferentes setores, permitindo simultaneamente alguma especificidade setorial.

Terceira etapa — **Desenvolvimento de um quadro de governação.**

Para ser eficiente e eficaz, o quadro de governação deve ter como base as principais partes interessadas, as prioridades identificadas no processo de elaboração e as condicionantes e o contexto das estruturas políticas e administrativas nacionais. Convém que o quadro reporte diretamente ao nível político, para dispor de poder de decisão e capacidade de afetação de recursos, e poder beneficiar do contributo de peritos em cibersegurança e de partes interessadas do setor. O artigo 7.º, n.º 1, alínea b), da Diretiva SRI faz referência ao quadro de governação, exigindo especificamente que cumpra «*as funções e responsabilidades dos organismos governamentais e dos outros intervenientes relevantes*».

Quarta etapa — **Elaboração e revisão do projeto de estratégia.**

Nesta fase, o projeto de estratégia deverá ser elaborado e sujeito a um exame mediante uma análise dos pontos fortes e fracos, das oportunidades e ameaças (SWOT), que poderá definir a necessidade de proceder a uma revisão do conteúdo. Na sequência do reexame interno, deverá ter lugar a consulta das partes interessadas. Será essencial proceder também a uma consulta pública para salientar a importância da estratégia proposta junto do público, receber os contributos provenientes de todas as fontes possíveis e procurar apoio para a afetação dos recursos necessários para a posterior execução da estratégia.

Quinta etapa **– Adoção formal.**

Esta última etapa envolve a adoção formal a nível político com um orçamento favorável que reflita a importância que o Estado-Membro em causa atribui à cibersegurança. Para atingir os objetivos da Diretiva SRI, e na comunicação do documento de estratégia nacional à Comissão, nos termos do artigo 7.º, n.º 3, a Comissão incentiva os Estados-Membros a fornecerem informações sobre o orçamento. As autorizações em matéria de orçamento e dos recursos humanos necessários são absolutamente essenciais para a eficácia da aplicação da estratégia e da diretiva. A cibersegurança continua a ser um domínio relativamente recente e em rápida expansão da política pública, pelo que, na maior parte dos casos, são necessários novos investimentos, mesmo se a situação global das finanças públicas exigir cortes e poupanças.

É possível obter aconselhamento sobre o processo e o conteúdo de estratégias nacionais junto de diversas fontes públicas e académicas, como por exemplo, a ENISA[6], a UIT[7], a OCDE[8], o Fórum Global de Cibercompetências e a Universidade de Oxford[9].

[6] ENISA, *National Cyber-Security Strategy Good Practice* 2016. Disponível em: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Disponível em: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

2.4. Medidas concretas que os Estados-Membros devem adotar antes do termo do prazo de transposição.

Antes da adoção da Diretiva, quase todos os Estados-Membros[10] tinham já publicado documentos indicados como sendo ENC. O ponto 6 do presente anexo enumera as estratégias atualmente em vigor em cada Estado-Membro[11]. Estas incluem, geralmente, princípios, orientações e objetivos estratégicos e, em alguns casos, medidas específicas para reduzir os riscos relacionados com a cibersegurança.

Dado que algumas destas estratégias foram aprovadas antes da adoção da Diretiva SRI, podem não conter, necessariamente, todos os elementos previstos no artigo 7.º. Para garantir uma transposição correta, os Estados-Membros terão de proceder a uma análise das lacunas, cotejando o conteúdo das respetivas ENC com os sete requisitos distintos enumerados no artigo 7.º quanto aos setores enumerados no anexo II da Diretiva e aos serviços enumerados no anexo III. As lacunas identificadas podem ser colmatadas mediante a revisão das respetivas ENC existentes ou tomando a decisão de rever exaustivamente, de raiz, os princípios que sustentam as respetivas estratégias nacionais no âmbito da SRI. As orientações fornecidas anteriormente no que respeita ao processo de adoção das ENC são também relevantes para a revisão e atualização de ENC existentes.

A UIT vai também publicar, em 2017, um conjunto de ferramentas dedicado às estratégias nacionais de cibersegurança (ver apresentação em: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

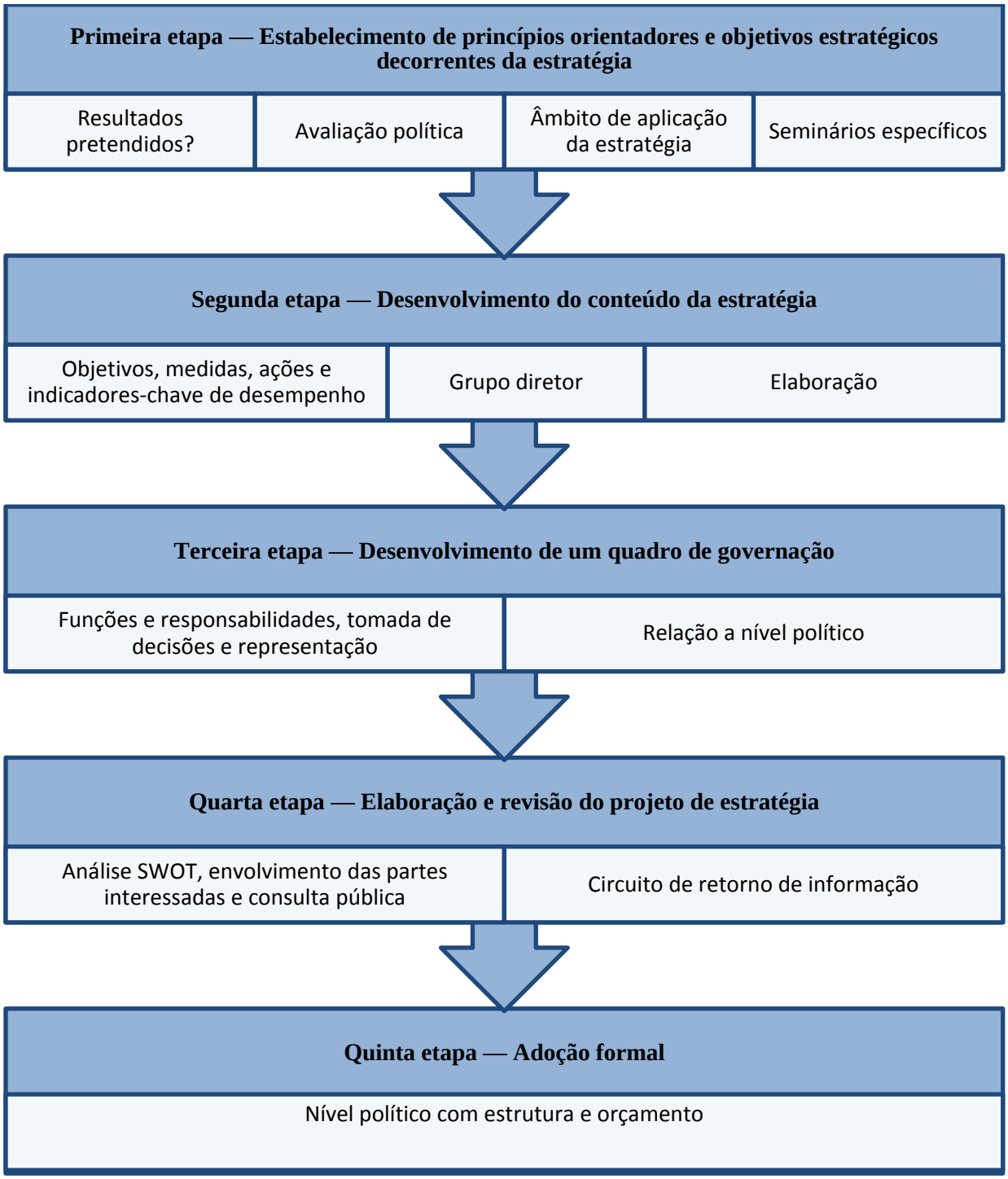
[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Disponível em: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Fórum Global de Cibercompetências e Universidade de Oxford, *Global Cyber Cybersecurity Capacity Maturity Model for Nations (CMM) — edição revista* (2016). Disponível em: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

[10] Exceto na Grécia, onde uma estratégia nacional de cibersegurança está em preparação desde 2014 (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Estas informações baseiam-se na síntese de ENC fornecida pela ENISA, no seguinte endereço: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Figura 1: Processo em cinco etapas para a adoção de uma ENC



3. Diretiva SRI: Autoridades nacionais competentes, pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (CSIRT).

Nos termos do artigo 8.º, n.º 1, os Estados-Membros devem designar uma ou mais autoridades nacionais competentes, que abranjam pelo menos os setores referidos no anexo II e os serviços referidos no seu anexo III da diretiva, encarregadas de acompanhar a aplicação da

diretiva. Os Estados-Membros podem atribuir esse papel a uma ou várias autoridades existentes.

Este ponto incide na forma como a Diretiva SRI reforça o grau de preparação dos Estados-Membros ao exigir que estes disponham de autoridades nacionais competentes e de equipas de resposta a incidentes de segurança informática (CSIRT) efetivas. Mais precisamente, o ponto abrange a obrigação de designar autoridades nacionais competentes, incluindo as atribuições do ponto de contacto único. Debruça-se sobre três temas: a) as possíveis estruturas nacionais de governação (por exemplo, modelos centralizados ou descentralizados, etc.) e outros requisitos; b) as atribuições do ponto de contacto único; c) as equipas de resposta a incidentes de segurança informática.

3.1. Tipo de autoridades.

O artigo 8.º da Diretiva SRI exige que os Estados-Membros designem autoridades nacionais competentes em matéria de segurança das redes e dos sistemas de informação, ao mesmo tempo que reconhece explicitamente a possibilidade de designar «*uma ou mais autoridades nacionais competentes*». O considerando 30 da diretiva explica esta opção política: «*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*».

Por conseguinte, os Estados-Membros são livres de optar por designar uma autoridade central responsável por todos os setores e serviços abrangidos pela diretiva ou várias autoridades, em função, por exemplo, do tipo de setor.

Ao decidir sobre a abordagem, os Estados-Membros podem recorrer à experiência nas abordagens nacionais seguidas no contexto da legislação em vigor sobre a proteção de infraestruturas críticas da informação (PICI). Tal como descrito no quadro 1, no caso da PICI, os Estados-Membros decidiram adotar uma abordagem centralizada ou uma abordagem descentralizada, ao atribuírem competências a nível nacional. Neste caso, os exemplos nacionais são apenas utilizados a título ilustrativo e com vista a chamar a atenção dos Estados-Membros para os quadros organizacionais existentes. Assim, isto não implica que a Comissão considere que o modelo utilizado pelos respetivos países para a PICI deva ser necessariamente utilizado para efeitos de transposição da Diretiva SRI.

Os Estados-Membros podem também optar por vários regimes híbridos que envolvam elementos de ambas as abordagens, centralizada e descentralizada. A escolha pode ser feita em sintonia com disposições nacionais anteriores em matéria de governação para os diferentes setores e serviços abrangidos pela diretiva, ou recentemente determinadas pelas autoridades competentes e pelas partes interessadas pertinentes identificadas como operadores de serviços essenciais e prestadores de serviços digitais. A existência de conhecimentos especializados em matéria de cibersegurança, critérios de atribuição de recursos, as relações entre as partes

interessadas e os interesses nacionais (por exemplo, o desenvolvimento económico, a segurança pública, etc.), podem também constituir fatores importantes conducentes às escolhas feitas pelos Estados-Membros.

3.2. Publicidade e aspetos pertinentes adicionais.

Nos termos do artigo 8.º, n.º 7, os Estados-Membros devem informar a Comissão sobre a designação de autoridades nacionais competentes e respetivas atribuições. Tal deve ser feito até ao termo do prazo de transposição.

Os artigos 15.º e 17.º da Diretiva SRI exigem que os Estados-Membros assegurem que as autoridades competentes disponham de poderes e meios específicos para executarem as atribuições enunciadas nesses artigos.

Além disso, a designação de entidades específicas como autoridades nacionais competentes deve ser tornada pública. A diretiva não especifica como essa divulgação deve ser efetuada. Uma vez que o objetivo deste requisito consiste em alcançar um elevado nível de sensibilização dos intervenientes abrangidos pela SRI e do público em geral, e com base na experiência adquirida noutros setores (telecomunicações, banca, medicamentos), a Comissão considera que esse objetivo poderia ser cumprido, por exemplo, pela criação de um portal amplamente divulgado.

O artigo 8.º, n.º 5, da Diretiva SRI exige que essas autoridades disponham de «recursos adequados» para executarem as atribuições que lhes são conferidas pela diretiva.

Quadro 1: Abordagens nacionais em matéria de proteção de infraestruturas críticas da informação (PICI).

Em 2016, a ENISA publicou um estudo[12] sobre as diferentes abordagens que os Estados-Membros seguem para proteger as respetivas infraestruturas críticas da informação. Existem dois perfis descritos no que se refere à governação da PICI nos Estados-Membros e que podem ser utilizados no contexto da transposição da Diretiva SRI.

Perfil 1: Abordagem descentralizada — com várias autoridades setoriais competentes para determinados setores e serviços enumerados nos anexos II e III da diretiva.

A abordagem descentralizada caracteriza-se:

(i) pelo princípio da subsidiariedade,
(ii) pela cooperação sólida entre organismos públicos,
(iii)pela legislação de âmbito setorial.

Princípio da subsidiariedade.

Em vez de estabelecer ou designar um único organismo com responsabilidade geral, a abordagem descentralizada segue o princípio da subsidiariedade. Isto significa que a responsabilidade pela execução cabe a uma autoridade setorial, que conhece melhor o setor local e mantém uma relação próxima com as partes interessadas. De acordo com este princípio, as decisões são tomadas por aqueles que estão mais próximos das pessoas afetadas.

Cooperação sólida entre organismos públicos.

Dada a variedade de organismos públicos envolvidos na PICI, muitos Estados-Membros criaram regimes de cooperação, a fim de coordenar o trabalho e os esforços das diferentes autoridades. Os referidos regimes de cooperação podem assumir a forma de redes informais ou de fóruns ou convénios mais institucionalizados. No entanto, estes regimes de cooperação servem apenas para o intercâmbio de informações e para a coordenação entre os diferentes organismos públicos, sem que possuam qualquer autoridade sobre os mesmos.

Legislação de âmbito setorial.

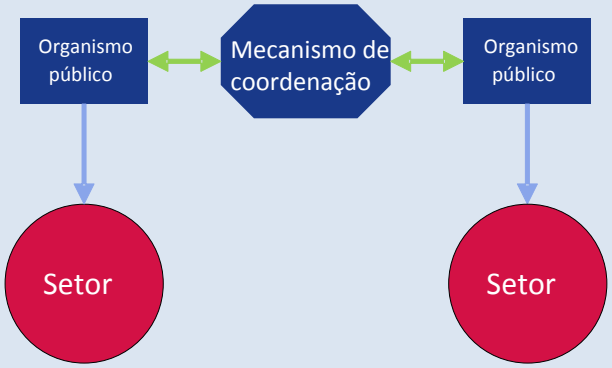
Os países que seguem a abordagem descentralizada em setores críticos abstêm-se frequentemente de legislar no domínio da PICI. Em vez disso, as disposições legislativas e regulamentares adotadas continuam a cingir-se ao âmbito setorial e, por conseguinte, podem variar significativamente entre setores. Esta abordagem tem a vantagem de harmonizar as medidas relacionadas com a SRI com os regulamentos setoriais existentes, para melhorar a aceitação pelo setor, bem como a eficácia da aplicação por parte da autoridade em causa.

Uma abordagem puramente descentralizada contém um risco substancial de redução da coerência na aplicação da diretiva entre os vários setores e serviços. Neste caso, a Diretiva

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Disponível em: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

prevê um ponto de contacto único a nível nacional para estabelecer ligações sobre questões transfronteiriças, podendo esta entidade ser também incumbida, pelo Estado-Membro em causa, da coordenação interna e da cooperação entre as várias autoridades nacionais competentes, em conformidade com o artigo 10.º da Diretiva.

Figura 2 — Abordagem descentralizada.



Exemplos de abordagens descentralizadas.

A Suécia é um bom exemplo de um país que segue uma abordagem descentralizada à PICI. O país utiliza uma «perspetiva sistémica», o que significa que as principais tarefas de PICI, tais como a identificação de serviços essenciais e de infraestruturas críticas, a coordenação e o apoio de operadores, as funções reguladoras, bem como as medidas de preparação para situações de emergência são da responsabilidade de diferentes organismos e municípios. Entre estes organismos contam-se a Agência de Proteção Civil da Suécia (MSB), o Organismo de Correios e Telecomunicações (PTS) e diversos organismos militares, de defesa e de aplicação da lei.

A fim de coordenar as ações entre os diferentes organismos e entidades públicas, o Governo sueco desenvolveu uma rede de cooperação constituída por autoridades «com responsabilidades específicas em matéria de segurança da sociedade da informação». Este Grupo de Cooperação para a Segurança da Informação (SAMFI) é composto por representantes das diferentes autoridades e reúne-se várias vezes por ano, para debater questões relacionadas com a segurança da informação nacional. As áreas temáticas do SAMFI encontram-se principalmente nos domínios político-estratégicos e abrangem temas como as questões técnicas e a normalização, o desenvolvimento, a nível nacional e internacional, no domínio da segurança da informação, ou a gestão e prevenção de incidentes informáticos. [Agência de Proteção Civil da Suécia (MSB) 2015].

A Suécia não publicou legislação central para a PICI, aplicável aos operadores de infraestruturas críticas da informação (ICI) em todos os setores. Em vez disso, a adoção de legislação que preveja obrigações para as empresas em determinados setores é da

responsabilidade das respetivas autoridades públicas. Por exemplo, a MSB tem o direito de emitir regulamentações para as autoridades governamentais no domínio da segurança da informação, ao passo que o PTS pode exigir aos operadores que apliquem determinadas medidas técnicas ou organizativas de segurança com base no direito derivado.

Outro exemplo de um país que apresenta características deste perfil é a Irlanda. A Irlanda segue uma «doutrina de subsidiariedade», segundo a qual cada ministério é responsável pela identificação das ICI e pela avaliação dos riscos no seu próprio setor. Além disso, não foi promulgada regulamentação específica em matéria de PICI. A legislação continua a ser setorial e existe principalmente para o setor da energia e das telecomunicações (2015). Outros exemplos são a Áustria, o Chipre e a Finlândia.

Perfil 2: Abordagem centralizada — com uma autoridade central competente para todos os setores e serviços enumerados nos anexos II e III da diretiva.

A abordagem centralizada caracteriza-se:

i) por ter uma autoridade central para vários setores,
ii) pela legislação abrangente.

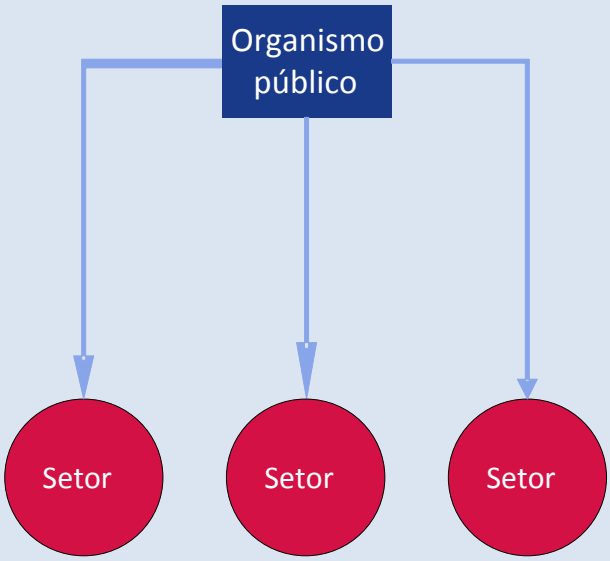
Autoridade central para vários setores.

Os Estados-Membros que seguem uma abordagem centralizada criaram autoridades com responsabilidades e competências alargadas em vários ou em todos os setores críticos, ou alargaram as competências das autoridades já existentes. Estas autoridades principais para a PICI combinam várias atribuições, como a preparação de planos de contingência, a gestão de situações de emergência, funções reguladoras e o apoio a operadores privados. Em muitos casos, as CSIRT nacionais ou governamentais integram a principal autoridade em matéria de PICI. Uma autoridade central tende a possuir uma maior concentração de conhecimentos especializados em matéria de cibersegurança do que várias autoridades setoriais, dada a escassez global de competências neste domínio.

Legislação abrangente.

A existência de um quadro legislativo abrangente cria obrigações e requisitos para todos os operadores de ICI em todos os setores. Este objetivo pode ser atingido graças a novas leis-quadro, ou completando regulamentação setorial já existente. Esta abordagem permitiria uma aplicação coerente da Diretiva SRI em todos os setores e serviços abrangidos. Evitar-se-ia, assim, o risco de lacunas de execução que poderão surgir no caso de existirem várias autoridades com responsabilidades específicas.

Figura 3 — Abordagem centralizada.



Exemplos de abordagens centralizadas.

A França é um bom exemplo de um Estado-Membro da UE com uma abordagem centralizada. A *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) foi declarada a principal autoridade nacional francesa de defesa dos sistemas de informação em 2011. A ANSSI tem uma função de supervisão importante em relação aos «operadores de importância vital» (OIV): a agência pode ordenar aos OIV que cumpram as medidas de segurança e está habilitada a realizar auditorias de segurança aos mesmos. Além disso, é o principal ponto de contacto único para os OIV, que são obrigados a comunicar os incidentes de segurança à agência.

Nos casos de incidentes de segurança, a ANSSI atua como o organismo responsável pelos planos de contingência para a PICI e decide sobre as medidas que os operadores devem tomar para dar resposta à crise. As ações do governo são coordenadas no centro de operações da ANSSI. A deteção de ameaças e a resposta a incidentes a nível operacional é efetuada pela CERT-FR, que faz parte da ANSSI.

A França criou um quadro jurídico abrangente para a PICI. Em 2006, o primeiro-ministro ordenou a elaboração de uma lista de setores de infraestruturas críticas. Com base nesta lista, que identificou doze setores vitais, o governo definiu cerca de 250 OIV. Em 2013, foi promulgada a Lei de Programação Militar[13]. Esta lei estabelece obrigações diferentes para os OIV, tais como a comunicação de incidentes ou a aplicação de medidas de segurança. Estes requisitos são obrigatórios para todos os OIV em todos os setores (Senado francês, 2013).

[13] *Loi de programmation militaire*.

3.3. Diretiva SRI, artigo 9.º: Equipas de resposta a incidentes de segurança informática (CSIRT).

Nos termos do artigo 9.º, os Estados-Membros devem designar uma ou mais CSIRT incumbidas de fazer face aos riscos e incidentes que afetem os setores enumerados no anexo II e os serviços enumerados no anexo III da Diretiva SRI. Tendo em conta o requisito de harmonização mínima consagrado no artigo 3.º da diretiva, os Estados-Membros têm a liberdade de utilizar as CSIRT também para outros setores não abrangidos pela diretiva, como a administração pública.

Os Estados-Membros podem decidir criar uma CSIRT no âmbito da autoridade nacional competente.[14].

3.4. Atribuições e requisitos.

As atribuições das CSIRT designadas, enunciadas no anexo I da Diretiva SRI, incluem:

- Monitorizar os incidentes a nível nacional;
- Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às partes interessadas relevantes sobre riscos e incidentes,
- Intervir em caso de incidentes;
- Proceder à análise dinâmica dos riscos e incidentes e ter uma visão geral da situação; e
- Participar na rede de CSIRT nacionais (rede de CSIRT) criada ao abrigo do artigo 12.º.

O artigo 14.º, n.os 3, 5 e 6, e o artigo 16.º, n.os 3, 6 e 7, enunciam tarefas específicas adicionais em relação às notificações de incidentes, caso um Estado-Membro decida que as CSIRT, além ou em vez das autoridades nacionais competentes, podem realizar essas funções.

Na transposição da diretiva, os Estados-Membros dispõem de opções relativamente às atribuições das CSIRT no que respeita aos requisitos de notificação de incidentes. É possível optar pela comunicação direta obrigatória às CSIRT, com vantagens em termos de eficiência administrativa; em alternativa, os Estados-Membros podem decidir-se pela comunicação direta às autoridades nacionais competentes, tendo as CSIRT o direito de acesso às informações comunicadas. Em última análise, as CSIRT estão envolvidas na resolução de problemas de dissuasão, deteção, resposta a ciberincidentes e atenuação do seu impacto (incluindo os não críticos, que não estão abrangidos pela obrigatoriedade de comunicação) junto das respetivas partes interessadas, estando a conformidade com os requisitos regulamentares sob a alçada das autoridades nacionais competentes.

Nos termos do artigo 9.º, n.º 3, da diretiva, os Estados-Membros devem também assegurar que as CSIRT em causa tenham acesso a infraestruturas de comunicação e informação seguras e resilientes.

[14] Ver artigo 9.º, n.º 1, última frase.

O artigo 9.º, n.º 4, da Diretiva exige que os Estados-Membros informem a Comissão sobre o mandato e sobre os principais elementos relativos ao processo de tratamento de incidentes das CSIRT designadas.

Os requisitos aplicáveis às CSIRT designadas pelos Estados-Membros estão previstos no anexo I da Diretiva SRI. As CSIRT devem garantir a ampla disponibilidade dos seus serviços de comunicações. As suas instalações e os sistemas informáticos de apoio devem estar situados em locais seguros e devem ser capazes de assegurar a continuidade das operações. Além disso, as CSIRT devem poder participar em redes de cooperação internacional.

3.5. Apoio à criação de CIRTS.

O programa de infraestruturas de serviços digitais (ISD) em matéria de cibersegurança, no âmbito do Mecanismo Interligar a Europa (MIE), pode conceder financiamentos substanciais da UE para ajudar as CSIRT dos Estados-Membros a melhorarem as suas capacidades e a colaborarem entre si por meio de um mecanismo de cooperação para o intercâmbio de informações. O mecanismo de cooperação, em fase de desenvolvimento ao abrigo do projeto SMART 2015/1089, destina-se a promover uma cooperação operacional célere e eficaz, a título voluntário, entre as CSIRT dos Estados-Membros, nomeadamente para apoiar as tarefas confiadas à rede de CSIRT ao abrigo do artigo 12.º da diretiva.

As informações pormenorizadas sobre os convites à apresentação de propostas relevantes para o reforço das capacidades das CSIRT dos Estados-Membros encontram-se disponíveis no sítio na Internet da Agência de Execução para a Inovação e as Redes (INEA) da Comissão Europeia[15].

O órgão de gestão das ISD em matéria de cibersegurança no âmbito do MIE proporciona uma estrutura informal para a prestação de orientações e assistência a nível político às CSIRT dos Estados-Membros para efeitos de reforço das capacidades e para a aplicação do mecanismo voluntário de cooperação.

As CSIRT criadas recentemente ou as CSIRT designadas para o desempenho das atribuições que constam do anexo I da Diretiva SRI podem contar com o aconselhamento e os conhecimentos da ENISA para melhorarem o seu desempenho e realizarem eficazmente as suas atividades[16]. A este respeito, vale a pena referir que as CSIRT dos Estados-Membros podem tomar como referência parte do trabalho recentemente realizado pela ENISA. Em especial, conforme indicado no ponto 7 do presente anexo, a Agência publicou um conjunto de documentos e estudos que descrevem boas práticas, recomendações a nível técnico, que incluem avaliações dos níveis de maturidade das CSIRT no que respeita às capacidades e aos serviços prestados por diversas CSIRT. Além disso, foram igualmente partilhadas orientações

[15] Disponível em: https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Ver artigo 9.º, n.º 5, da Diretiva SRI.

e boas práticas por redes de CSIRT, tanto a nível mundial (FIRST[17]) como a nível europeu (Trusted Introducer, TI[18]).

3.6. O papel dos pontos de contacto únicos.

Nos termos do artigo 8.º, n.º 3, da Diretiva SRI, cada Estado-Membro deve designar um ponto de contacto único nacional, que exercerá uma função de ligação para assegurar a cooperação transfronteiriça com as autoridades competentes de outros Estados-Membros, e com o grupo de cooperação e a rede de CSIRT[19] criada pela própria diretiva. O considerando 31 e o artigo 8.º, n.º 4, explicam o *fundamento* deste requisito, ou seja, facilitar a cooperação e comunicação transfronteiriças. Isto é particularmente necessário, uma vez que os Estados-Membros podem decidir ter mais do que uma autoridade nacional. Assim, a existência de um ponto de contacto único facilitará a identificação e a cooperação entre autoridades de diferentes Estados-Membros.

O papel de ligação do ponto de contacto único pode envolver uma interação com os secretariados do grupo de cooperação e da rede de CSIRT nos casos em que o ponto de contacto único nacional não é uma CSIRT nem um membro do grupo de cooperação. Além disso, os Estados-Membros devem assegurar que o ponto de contacto único seja informado sobre as notificações recebidas dos operadores de serviços essenciais e dos prestadores de serviços digitais[20].

O artigo 8.º, n.º 3, da diretiva especifica que, no caso de um Estado-Membro adotar uma abordagem centralizada, ou seja, designar uma única autoridade competente, essa autoridade assumirá também as funções de ponto de contacto único. Se um Estado-Membro optar por uma abordagem descentralizada, poderá escolher uma das diferentes autoridades competentes para exercer as funções de ponto único de contacto. Independentemente do modelo institucional escolhido, sempre que uma autoridade competente, a CSIRT e o ponto de contacto único forem entidades distintas, o Estado-Membro tem a obrigação de assegurar uma cooperação efetiva entre estas, a fim de cumprirem as obrigações previstas na diretiva[21].

O ponto de contacto único é obrigado a apresentar até 9 de agosto de 2018 e, posteriormente, uma vez por ano, um relatório de síntese ao grupo de cooperação sobre as notificações recebidas, que deve incluir o número de notificações, a natureza dos incidentes e as medidas tomadas pelas autoridades, tais como informar outros Estados-Membros afetados sobre o incidente, ou prestar informações pertinentes à empresa notificante para o tratamento do incidente em causa[22]. A pedido da autoridade competente ou da CSIRT, o ponto de contacto único tem de transmitir as notificações dos operadores de serviços essenciais aos pontos de contacto únicos dos outros Estados-Membros afetados por esses incidentes[23].

---

[17] Fórum das equipas de segurança e de resposta a incidentes (https://www.first.org/).
[18] https://www.trusted-introducer.org/.
[19] Rede de CSIRT nacionais para a cooperação operacional entre Estados-Membros, ao abrigo do artigo 12.º.
[20] Ver artigo 10.º, n.º 3.
[21] Ver o artigo 10.º, n.º 1.
[22] Idem.
[23] Ver artigo 14.º, n.º 5.

Os Estados-Membros devem informar a Comissão sobre a designação do ponto de contacto único e as suas atribuições até ao termo do prazo de transposição. A designação do ponto de contacto único deve ser tornada pública, da mesma forma que as autoridades nacionais competentes. A Comissão deve publicar a lista dos pontos de contacto únicos designados.

3.7. Sanções.

O artigo 21.º confere margem aos Estados-Membros para decidirem sobre o tipo e a natureza das sanções aplicáveis, desde que sejam efetivas, proporcionadas e dissuasivas. Por outras palavras, os Estados-Membros têm, em princípio, liberdade para decidir sobre o montante máximo das sanções previstas na respetiva legislação nacional, mas o montante ou a percentagem escolhida deve permitir às autoridades nacionais aplicar, em cada caso concreto, sanções efetivas, proporcionadas e dissuasivas, tendo em conta diversos fatores, como a frequência ou a gravidade da infração.

4. Entidades sujeitas a obrigações em matéria de requisitos de segurança e de notificação de incidentes.

As entidades que desempenham um papel importante para a sociedade e para a economia, referidas no artigo 4.º, n.os 4 e 5, da diretiva como operadores de serviços essenciais e prestadores de serviços digitais, devem adotar medidas de segurança adequadas e notificar incidentes graves às autoridades nacionais competentes. Tal *justifica-se* porque o impacto dos incidentes de segurança em tais serviços pode constituir uma grave ameaça para o funcionamento dos mesmos, o que pode provocar grandes perturbações nas atividades económicas e na sociedade em geral, eventualmente minar a confiança dos utilizadores e causar graves prejuízos à economia da União[24].

O presente ponto apresenta uma panorâmica geral das entidades incluídas no âmbito de aplicação dos anexos II e III da Diretiva SRI, e enumera as suas obrigações. A identificação dos operadores de serviços essenciais é abordada de forma exaustiva, dada a importância deste processo para a execução harmonizada da Diretiva SRI em toda a UE. Também apresenta explicações exaustivas relativamente às definições de infraestruturas digitais e de prestadores de serviços digitais. Examina, ainda, a eventual inclusão de outros setores e explica melhor a abordagem específica no que respeita aos prestadores de serviços digitais.

4.1. Operadores de serviços essenciais.

A Diretiva SRI não define explicitamente as entidades específicas que, no âmbito da sua aplicação, serão consideradas operadores de serviços especiais. Em vez disso, estabelece os critérios que os Estados-Membros deverão aplicar para realizarem um processo de identificação que, em última análise, determinará que empresas individuais pertencentes ao tipo de entidades enumeradas no anexo II serão consideradas operadores de serviços essenciais, e, por conseguinte, ficarão sujeitas às obrigações que decorrem da diretiva.

[24] Ver considerando 2.

4.1.1. Tipo de entidades enumeradas no anexo II da Diretiva SRI.

O artigo 4.º, n.º 4, define um OES como 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. No anexo II, são enumerados os setores, subsetores e o tipo de entidades em relação aos quais cada Estado-Membro deve proceder a um processo de identificação nos termos do artigo 5.º, n.º 2[25]. Os setores incluem a energia, os transportes, a banca, as infraestruturas dos mercados financeiros, a saúde, a água e as infraestruturas digitais.

Em relação à maioria das entidades que pertencem a «setores tradicionais», a legislação da UE contém definições bem desenvolvidas, a que o anexo II faz referência. No entanto, em relação ao setor das infraestruturas digitais, enumeradas no ponto 7 do anexo II, incluindo os pontos de troca de tráfego, os sistemas de nomes de domínio e os registos de nomes de domínios de topo, não é esse o caso. Por conseguinte, com o objetivo de esclarecer estas definições, segue-se uma explicação pormenorizada das mesmas.

1) Ponto de troca de tráfego (IXP).

O termo ponto de troca de tráfego é definido no artigo 4.º, n.º 13, e clarificado de forma mais pormenorizada no considerando 18, e pode ser descrito como uma estrutura de rede que permite a interligação de mais de dois sistemas autónomos tecnicamente independentes, sobretudo a fim de facilitar a troca de tráfego na Internet. O ponto de troca de tráfego também pode ser descrito como um local físico onde várias redes podem proceder à troca de tráfego na Internet entre si através de um comutador. O principal objetivo de um ponto de troca de tráfego consiste em permitir a interligação direta de redes, por meio da troca, em vez do recurso a uma ou mais redes de terceiros. O operador de um ponto de troca de tráfego não é, em princípio, responsável pelo encaminhamento do tráfego na Internet. O encaminhamento do tráfego é efetuado pelos fornecedores de serviços de rede. As vantagens da interligação direta são numerosas, mas as principais razões são os custos, a latência e a largura de banda. O tráfego que passa por um ponto de troca geralmente não é faturado por qualquer das partes, ao passo que o tráfego para um fornecedor de serviços de Internet a montante é pago. A interligação direta, frequentemente situada na mesma cidade que ambas as redes, evita a necessidade de os dados percorrerem longas distâncias para chegarem de uma rede a outra, reduzindo assim a latência.

É de salientar que a definição de ponto de troca de tráfego não abrange os pontos físicos em que apenas duas redes físicas se interligam (ou seja, os fornecedores de serviços de rede, como a BASE e a Proximus, na Bélgica). Por conseguinte, ao transpor a diretiva, os Estados-Membros devem estabelecer uma distinção entre os operadores que estão a facilitar a troca de tráfego agregado na Internet entre vários operadores de rede e os operadores de rede únicos, que interligam fisicamente as suas redes com base num acordo de interligação. Neste último caso, os fornecedores de serviços de rede não estão abrangidos pela definição do artigo 4.º,

[25] Para informações mais pormenorizadas sobre o processo de identificação, consultar o ponto 4.1.6.

n.º 13. O considerando 18 esclarece esta questão, ao referir que os pontos de troca de tráfego não proporcionam o acesso à rede nem atuam como prestadores ou operadores de tráfego. A última categoria de fornecedores são as empresas que oferecem redes e/ou serviços de comunicações públicas que estejam sujeitas a obrigações em matéria de segurança e notificação previstas nos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE, e que, por conseguinte, estão excluídas do âmbito de aplicação da Diretiva SRI[26].

2) Sistema de nomes de domínio (DNS).

O termo «sistema de nomes de domínio» é definido no artigo 4.º, n.º 14, como «*um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio*». Mais precisamente, o DNS pode ser descrito como um sistema de gestão de nomes distribuído e hierárquico para computadores, serviços ou quaisquer outros recursos ligados à Internet, que permite a codificação de nomes de domínio para endereços IP (protocolo Internet). A principal função do sistema consiste em traduzir os nomes de domínio atribuídos para endereços IP. Para este efeito, o DNS explora uma base de dados e utiliza servidores e resolvedores de nomes para permitir este tipo de «tradução» dos nomes de domínio para endereços IP operacionais. Apesar de a codificação dos nomes de domínio não ser a única responsabilidade do DNS, é uma das funções fundamentais do sistema. A definição legal prevista no artigo 4.º, n.º 14, incide sobre o principal papel do sistema do ponto de vista do utilizador, sem entrar em pormenores mais técnicos, como, por exemplo, o funcionamento do espaço dos nomes de domínio, dos servidores de nomes, dos resolvedores, etc.. Por último, o artigo 4.º, n.º 15, esclarece quem deve ser considerado como um prestador de serviços de DNS.

3) Registo de nomes de domínio de topo (registo de nomes de TLD).

O registo de nomes de domínio de topo é definido no artigo 4.º, n.º 16, como uma entidade que administra e opera o registo de nomes de domínio da Internet no contexto de um domínio de topo específico. Essa administração e gestão dos nomes de domínio inclui a codificação de nomes de domínio de topo para endereços IP.

A Autoridade para a Atribuição dos Números Internet (IANA) é responsável pela coordenação, a nível mundial, do sistema de raiz do DNS, da atribuição de endereços do protocolo Internet e de outros recursos do protocolo Internet. Em especial, a IANA é responsável pela atribuição de domínios de topo genéricos (gTLD), por exemplo, o domínio «.com», e de domínios de topo com código de país (ccTLD), por exemplo, o domínio «.be», aos operadores (registos) e pela manutenção dos respetivos dados técnicos e administrativos. A IANA mantém um registo global de TLD atribuídos e desempenha um papel importante na promulgação desta lista a utilizadores de Internet em todo o mundo, bem como na introdução de novos TLD.

[26] Para mais informações, ver ponto 5.2 sobre a relação entre a Diretiva SRI e a Diretiva 2002/21/CE.

Uma tarefa importante dos registos é atribuir nomes de domínio segundo nível aos chamados registantes, abaixo dos respetivos TLD. Esses registantes também têm a possibilidade de, por sua iniciativa, atribuírem nomes de domínio de terceiro nível, se assim o pretenderem. Os ccTLD são concebidos para representarem um país ou um território com base na norma ISO 3166-1. Os TLD «genéricos» não têm, em geral, uma designação geográfica ou de país.

Importa observar que a exploração do registo de nomes de domínio de topo pode incluir a disponibilização do DNS. Por exemplo, de acordo com as regras da IANA em matéria de delegação, a entidade designada que trata dos ccTLD deve, *inter alia*, supervisionar os nomes de domínio e operar o DNS desse país[27]. Os Estados-Membros devem ter em conta essas circunstâncias ao procederem à identificação dos operadores de serviços essenciais ao abrigo do artigo 5.º, n.º 2.

4.1.2. Identificação de operadores de serviços essenciais.

Em conformidade com os requisitos estabelecidos no artigo 5.º da diretiva, cada Estado-Membro deve efetuar um processo de identificação de todas as entidades dos tipos enumerados no anexo II que estejam estabelecidas no respetivo território. Em resultado desta avaliação, todas as entidades que cumpram os critérios estabelecidos no artigo 5.º, n.º 2, devem ser identificadas como operadores de serviços especiais e ficar sujeitas aos requisitos de segurança e de notificação previstos no artigo 14.º.

Os Estados-Membros têm de identificar os operadores de cada setor e subsetor até 9 de novembro de 2018. A fim de apoiar os Estados-Membros ao longo deste processo, o grupo de cooperação está atualmente a elaborar um documento de orientação com informações pertinentes sobre as medidas necessárias e as melhores práticas relacionadas com a identificação de operadores de serviços especiais.

Além disso, em conformidade com o artigo 24.º, n.º 2, o grupo de cooperação discutirá o processo, o conteúdo e o tipo de medidas nacionais que permitam identificar os operadores de serviços essenciais em setores específicos. Um Estado-Membro pode, antes de 9 de novembro de 2018, procurar discutir o seu projeto de medidas nacionais que permitam identificar os operadores de serviços essenciais no âmbito do grupo de cooperação.

4.1.3. Inclusão de outros setores.

Tendo em conta o requisito de harmonização mínima consagrado no artigo 3.º, os Estados-Membros podem adotar ou manter legislação que garanta um nível mais elevado de segurança das redes e dos sistemas de informação. Neste contexto, os Estados-Membros têm, no geral, liberdade para alargar as obrigações em matéria de segurança e de notificação previstas no artigo 14.º a entidades pertencentes a outros setores e subsetores que não os enumerados no anexo II da Diretiva SRI. Vários Estados-Membros decidiram ou estão a ponderar a inclusão de alguns dos seguintes setores:

i) Administrações públicas

[27] Informação disponível em: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

As administrações públicas podem prestar serviços essenciais referidos no anexo II da diretiva que cumpram os requisitos estabelecidos no artigo 5.º, n.º 2. Em tais casos, as administrações públicas que prestam esses serviços serão abrangidas pelos requisitos de segurança e notificação pertinentes. Ao invés, quando as administrações públicas prestam serviços que não se enquadram no âmbito de aplicação acima referido, esses serviços não serão abrangidos pelos requisitos em questão.

As administrações públicas são responsáveis pela correta execução dos serviços públicos prestados por órgãos governamentais, autoridades regionais e locais, organismos e empresas associadas. Estes serviços implicam, frequentemente, a criação e a gestão de dados pessoais e empresariais sobre indivíduos e organizações, que podem ser partilhados e disponibilizados a várias entidades públicas. De um modo mais geral, o elevado nível de segurança das redes e sistemas de informação utilizados pelas administrações públicas é de grande interesse para a sociedade e a economia como um todo. A Comissão considera, por conseguinte, que seria adequado que os Estados-Membros ponderassem incluir a administração pública no âmbito de aplicação da legislação nacional que transpõe a diretiva, além da prestação de serviços essenciais, tal como previsto no anexo II e no artigo 5.º, n.º 2.

ii) Setor postal

O setor postal inclui a prestação de serviços postais, como a recolha, triagem, transporte e distribuição dos objetos postais.

iii) Setor alimentar

O setor alimentar diz respeito à produção de produtos agrícolas e outros produtos alimentares e poderá incluir serviços essenciais, como a criação de condições de segurança alimentar e a garantia da qualidade e segurança dos alimentos.

iv) Indústria química e nuclear

A indústria química e nuclear refere-se, nomeadamente, à armazenagem, produção e transformação de produtos químicos e petroquímicos ou de materiais nucleares.

v) Setor do ambiente

As atividades no domínio do ambiente abrangem a disponibilização de bens e serviços necessários para proteger o ambiente e gerir recursos. Por conseguinte, as atividades destinam-se a prevenir, reduzir e eliminar a poluição, bem como a preservar as reservas de recursos naturais. No âmbito deste setor, os serviços essenciais podem ser a monitorização e o controlo da poluição (por exemplo, do ar e da água) e dos fenómenos meteorológicos.

vi) Proteção civil

O objetivo do setor da proteção civil consiste na prevenção, preparação e resposta a catástrofes naturais e de origem humana. Os serviços prestados para esse efeito podem ser a ativação de números de emergência e a realização de ações destinadas a informar sobre a contenção e a resposta a situações de emergência.

4.1.4. Competência jurisdicional.

Nos termos do artigo 5.º, n.º 1, cada Estado-Membro deve identificar os operadores de serviços especiais estabelecidos no respetivo território. A disposição não especifica a forma de estabelecimento legal, mas o considerando 21 esclarece que este pressupõe o exercício efetivo e real de uma atividade com base numa organização estável e que a forma jurídica dessa organização não deve ser um fator determinante. Isto significa que os Estados-Membros podem ter competência jurisdicional sobre um operador de serviços essenciais não apenas nos casos em que o operador tenha a sua sede social no seu território, mas também nos casos em que o operador tenha, por exemplo, uma sucursal ou outra forma de estabelecimento legal.

Esta situação tem como consequência que vários Estados-Membros possam ter, em simultâneo, competência jurisdicional sobre a mesma entidade.

4.1.5. Informações a apresentar à Comissão.

Para efeitos da avaliação que a Comissão tem de efetuar nos termos do artigo 23.º, n.º 1, da Diretiva SRI, os Estados-Membros devem apresentar à Comissão, até 9 de novembro de 2018, e posteriormente de dois em dois anos, as seguintes informações:

- As medidas nacionais que permitem identificar os operadores de serviços essenciais;
- A lista de serviços essenciais;
- O número de operadores de serviços essenciais identificados por cada setor referido no anexo II e a importância desses operadores para o setor; e
- Os limiares, caso existam, utilizados para determinar o nível de oferta em função do número de utilizadores que dependem desse serviço, tal como referido no artigo 6.º, n.º 1, alínea a), ou a importância da entidade, em conformidade com o artigo 6.º, n.º 1, alínea f).

A avaliação prevista no artigo 23.º, n.º 1, que precede a avaliação global da diretiva, reflete a importância que os colegisladores atribuem à correta transposição da diretiva, no que diz respeito à identificação dos operadores de serviços essenciais, para evitar a fragmentação do mercado.

A fim de levar a cabo este processo da melhor maneira possível, a Comissão incentiva os Estados-Membros a debaterem este assunto, bem como a trocarem experiências relevantes no âmbito do grupo de cooperação. Além disso, a Comissão incentiva os Estados-Membros a partilharem com a Comissão, se necessário a título confidencial, as listas de operadores de serviços essenciais identificados (que, em última análise, foram selecionados) além de todas as informações que os Estados-Membros, por força da diretiva, devem apresentar à Comissão. A disponibilidade dessas listas permitirá facilitar e contribuir para uma melhor qualidade da avaliação da Comissão sobre a coerência do processo de identificação, e permitirá comparar as abordagens entre os Estados-Membros, conduzindo assim a uma melhor consecução dos objetivos da diretiva.

4.1.6. Como proceder ao processo de identificação?

Tal como indicado na figura 4, existem seis questões-chave que as autoridades nacionais devem examinar ao realizarem o processo de identificação no respeitante a uma determinada entidade. Nos parágrafos que se seguem, cada questão corresponde a uma etapa que deverá ser cumprida em conformidade com o disposto no artigo 5.º, em conjugação com o artigo 6.º, e tendo também em conta a aplicabilidade do artigo 1.º, n.º 7.

Etapa 1 — **A entidade pertence a um setor ou subsetor e corresponde ao tipo abrangido pelo anexo II da diretiva?**

Uma autoridade nacional deve avaliar se uma entidade estabelecida no respetivo território pertence aos setores e subsetores enumerados no anexo II da diretiva. O anexo II abrange vários setores económicos que são considerados fundamentais para assegurar o bom funcionamento do mercado interno. O anexo II refere-se particularmente aos seguintes setores e subsetores:

- Energia: eletricidade, petróleo e gás
- Transportes: transporte aéreo, transporte ferroviário, transporte marítimo e por vias navegáveis interiores e transporte rodoviário
- Setor bancário: instituições de crédito
- Infraestruturas do mercado financeiro: plataformas de negociação, contrapartes centrais
- Saúde: prestadores de cuidados de saúde (nomeadamente hospitais e clínicas privadas)
- Água: fornecimento e distribuição de água potável
- Infraestruturas digitais: pontos de troca de tráfego, prestadores de serviços do sistema de nomes de domínio, registos de nomes de domínio de topo[28]

Etapa 2 — **Aplica-se uma *lex specialis*?**

Na etapa seguinte, a autoridade nacional deve analisar se a disposição referente à *lex specialis*, consagrada no artigo 1.º, n.º 7, é aplicável. Em particular, esta disposição prevê que, se houver um ato jurídico da UE que imponha requisitos de segurança e/ou de notificação aos prestadores de serviços digitais ou aos operadores de serviços essenciais que seja, pelo menos, equivalente aos requisitos correspondentes ao abrigo da Diretiva SRI, devem aplicar-se as obrigações ao abrigo do ato jurídico especial. Além disso, o considerando 9 esclarece que, se os requisitos previstos no artigo 1.º, n.º 7, forem cumpridos, os Estados-Membros devem aplicar as disposições do ato jurídico setorial da UE, nomeadamente as relativas à competência jurisdicional. Contrariamente, as disposições relevantes da Diretiva SRI não serão aplicáveis. Neste caso, a autoridade competente não deve prosseguir com o processo de identificação ao abrigo do artigo 5.º, n.º 2[29].

[28]Estas entidades são analisadas mais pormenorizadamente no ponto 4.1.1.

[29] No ponto 5.1, são apresentadas informações mais pormenorizadas sobre a aplicabilidade da *lex specialis*.

Etapa 3 — **O operador está a prestar um serviço essencial na aceção da diretiva?**

Nos termos do artigo 5.º, n.º 2, alínea a), a entidade sujeita à identificação deve prestar um serviço essencial para a manutenção de atividades sociais e/ou económicas cruciais. Ao proceder a esta avaliação, os Estados-Membros deverão ter em conta que uma entidade pode prestar em simultâneo serviços essenciais e não essenciais. Isto significa que os requisitos de segurança e notificação previstos na Diretiva SRI serão aplicáveis a um determinado operador apenas na extensão dos serviços essenciais que este prestar.

Em conformidade com o artigo 5.º, n.º 3, cada Estado-Membro deve elaborar uma lista de todos os serviços essenciais prestados por operadores de serviços especiais estabelecidos no respetivo território. A referida lista deve ser apresentada à Comissão até 9 de novembro de 2018 e, posteriormente, de dois em dois anos[30].

Etapa 4 — **O serviço depende de uma rede e sistema de informação?**

Além disso, deve ser indicado se este serviço preenche o segundo critério previsto no artigo 5.º, n.º 2, alínea b), e, em particular, se a prestação do serviço essencial depende de redes e sistemas de informação na aceção do artigo 4.º, n.º 1.

Etapa 5 — **Um incidente de segurança poderia ter um efeito perturbador importante?**

O artigo 5.º, n.º 2, alínea c), exige que a autoridade nacional determine se um incidente poderia ter um efeito perturbador importante na prestação do serviço. Neste contexto, o artigo 6.º, n.º 1, estabelece vários fatores transetoriais que devem ser tidos em conta nessa avaliação. Além disso, o artigo 6.º, n.º 2, estipula que a avaliação deve ter igualmente em conta, se adequado, fatores setoriais específicos.

Os **fatores transetoriais** enumerados no artigo 6.º, n.º 1, são os seguintes:

- O número de utilizadores que dependem dos serviços prestados pela entidade em causa;
- A dependência de outros setores referidos no anexo II em relação ao serviço prestado por essa entidade;
- O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais ou a segurança pública;
- A quota de mercado dessa entidade;
- A distribuição geográfica, no que se refere à zona que pode ser afetada por um incidente;
- 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.

No que diz respeito aos **fatores setoriais específicos**, o considerando 28 apresenta alguns exemplos (ver quadro 4), o que poderá fornecer orientações úteis às autoridades nacionais.

[30] Ver artigo 5.º, n.º 7, alínea b).

Quadro 4: Exemplos de fatores setoriais específicos a ter em conta na determinação de um efeito perturbador importante em caso de incidente.

Setor	Exemplos de fatores setoriais específicos
Fornecedores de energia	quantidade ou percentagem de energia nacional gerada
Fornecedores de petróleo	volume diário fornecido
Transporte aéreo (incluindo os aeroportos e as transportadoras aéreas) **Transporte ferroviário** **Portos marítimos**	percentagem de volume de tráfego nacional número de passageiros ou de operações de movimentação de carga anuais
Serviços bancários ou infraestruturas do mercado financeiro	importância sistémica com base nos ativos totais rácio ativos totais/PIB
Setor da saúde	número de pacientes sob cuidados do prestador em cada ano
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) existência de fontes alternativas de abastecimento de água que abranjam a mesma zona geográfica

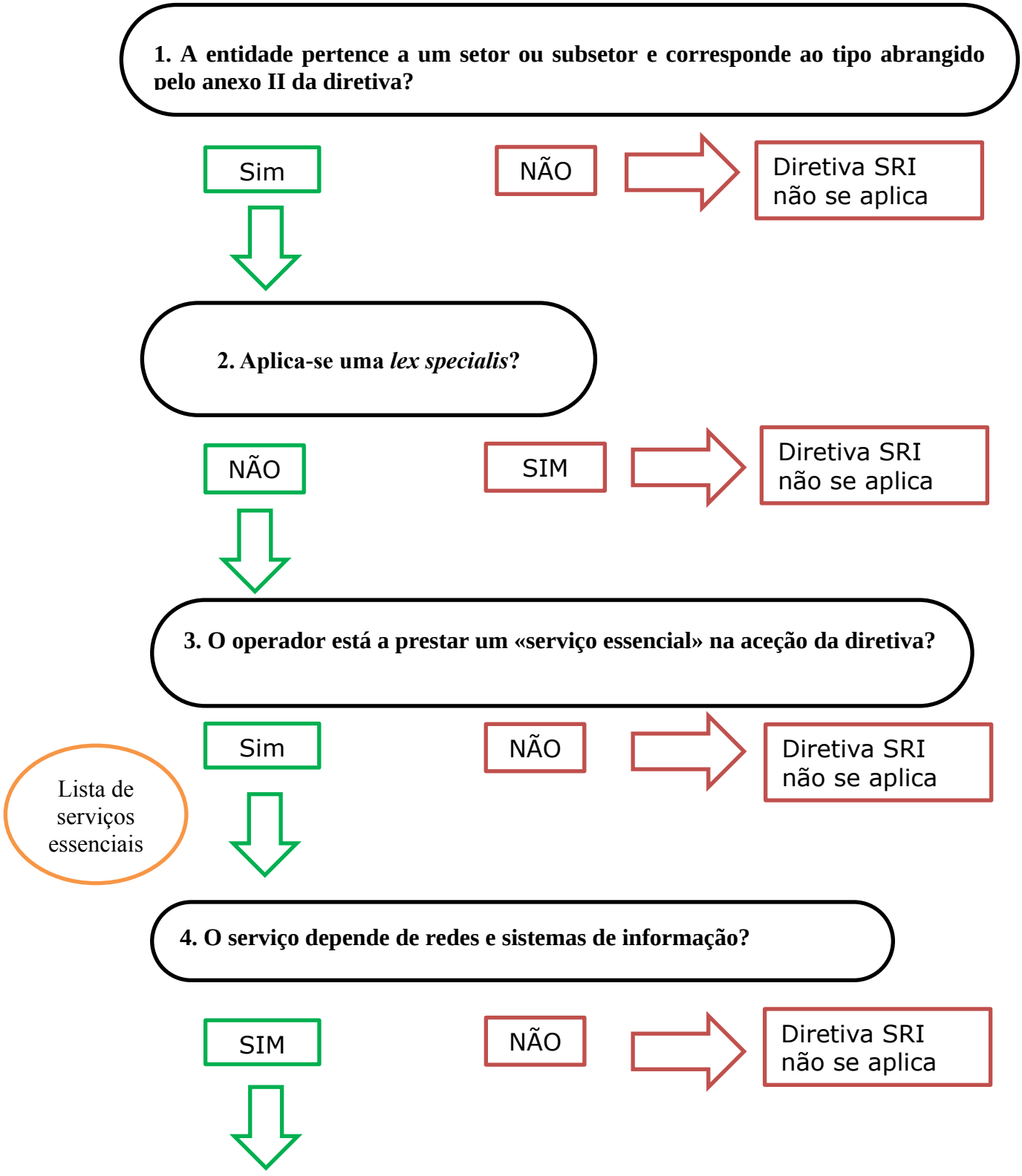
Importa salientar que, ao procederem à avaliação nos termos do artigo 5.º, n.º 2, os Estados-Membros não devem acrescentar outros critérios além dos enumerados na referida disposição, pois isso poderia reduzir o número de operadores de serviços especiais identificados e prejudicar a harmonização mínima em relação aos operadores em causa, consagrada no artigo 3.º da diretiva.

Etapa 6 **— O operador em causa presta serviços essenciais noutros Estados-Membros?**

A etapa 6 refere-se a casos em que o operador fornece os seus serviços essenciais em dois ou mais Estados-Membros. Antes da conclusão do processo de identificação, o artigo 5.º, n.º 4, exige que os Estados-Membros em causa iniciem um processo de consulta[31].

[31] Para mais informações sobre o processo de consulta, ver o ponto 4.1.7.

Figura 4: Processo de identificação em seis etapas.



5. Um incidente de segurança poderia ter um efeito perturbador importante?

Fatores transetoriais (artigo 6.º, n.º 1)

- **Número de utilizadores que dependem dos serviços**
- **Dependência** de outros setores essenciais em relação ao serviço
- Impacto que os incidentes poderão ter nas **atividades económicas e sociais** ou na **segurança pública**
- Possível **distribuição geográfica**
- Importância da entidade para a manutenção de um **nível** suficiente **do serviço**

id

Fatores setoriais específicos (exemplos referidos no considerando 28)

- **Energia**: quantidade ou percentagem de energia nacional gerada
- **Transportes**: percentagem de volume de tráfego nacional e número de operações anuais
- **Saúde**: número de pacientes sob cuidados do prestador em cada ano

Sim

NÃO → Diretiva SRI não se aplica

6. O operador em causa presta serviços essenciais noutros Estados-Membros?

SIM

NÃO → Diretiva SRI não se aplica

Consulta obrigatória do Estado-Membro em causa

Adoção de medidas nacionais (por exemplo, lista dos operadores de serviços essenciais, medidas políticas e jurídicas).

4.1.7. Processo de consulta transfronteiriço.

Caso um operador preste serviços essenciais em dois ou mais Estados-Membros, estes devem, nos termos do artigo 5.º, n.º 4, consultar-se mutuamente antes da conclusão do processo de identificação. O objetivo desta consulta consiste em facilitar a avaliação da natureza crítica do operador em termos de impacto transfronteiriço.

O resultado pretendido da consulta é que as autoridades nacionais envolvidas troquem argumentos e posições e, idealmente, cheguem ao mesmo resultado em relação à identificação do operador em causa. No entanto, a Diretiva SRI não impede que os Estados-Membros cheguem a conclusões diferentes sobre a identificação ou não de uma entidade como operador de serviços especiais. O considerando 24 refere a possibilidade de os Estados-Membros solicitarem a assistência do grupo de cooperação a este respeito.

No entender da Comissão, os Estados-Membros devem procurar obter um consenso sobre estas questões, a fim de evitar uma situação em que a mesma empresa se depara com estatutos jurídicos distintos em diferentes Estados-Membros. A divergência deve ser verdadeiramente excecional, por exemplo, nos casos em que uma entidade considerada operador de serviços especiais num Estado-Membro tem uma atividade marginal e irrelevante noutro Estado-Membro.

4.2. Requisitos de segurança.

Nos termos do artigo 14.º, n.º 1, os Estados-Membros devem assegurar que os operadores de serviços especiais, tendo em conta os conhecimentos técnicos disponíveis, 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 as organizações utilizam na prestação dos seus serviços. Em conformidade com o artigo 14.º, n.º 2, as medidas adequadas devem evitar e reduzir ao mínimo o impacto de um incidente.

Uma vertente específica do grupo de cooperação está atualmente a trabalhar na elaboração de orientações não vinculativas sobre as medidas de segurança para os operadores de serviços essenciais[32]. O documento de orientação deverá ser finalizado pelo grupo até ao quarto trimestre de 2017. A Comissão incentiva os Estados-Membros a seguirem atentamente o documento de orientação a elaborar pelo grupo de cooperação, de modo a que as disposições nacionais sobre requisitos de segurança estejam, tanto quanto possível, em sintonia. A harmonização desses requisitos facilitará em grande medida o cumprimento por parte dos operadores de serviços essenciais que frequentemente prestam serviços essenciais em mais do que um Estado-Membro e as funções de supervisão das autoridades nacionais competentes e das CSIRT.

[32] Para efeitos desta vertente de trabalho, foram distribuídas e utilizadas listas de normas internacionais, boas práticas e metodologias de avaliação/gestão dos riscos para todos os setores abrangidos pela Diretiva SRI como contributo para os domínios e as medidas propostas em matéria de segurança.

4.3 Requisitos de notificação.

Nos termos do artigo 14.º, n.º 3, os Estados-Membros devem assegurar que os operadores de serviços essenciais notifiquem «*os incidentes com um impacto importante na continuidade dos serviços essenciais*». Por conseguinte, os operadores de serviços essenciais não devem notificar pequenos incidentes, mas apenas incidentes graves que afetem a continuidade do serviço essencial. Nos termos do artigo 4.º, n.º 7, entende-se por incidente «um evento com um efeito adverso real na segurança das redes e dos sistemas de informação». O termo «segurança das redes e dos sistemas de informação» é definido, nos termos do artigo 4.º, n.º 2, como sendo «*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*.» Por conseguinte, um evento com um efeito adverso não apenas na disponibilidade, mas também na autenticidade, integridade ou confidencialidade dos dados ou dos serviços conexos pode determinar a obrigação de notificação. Com efeito, a continuidade do serviço, tal como referido no artigo 14.º, n.º 3, pode ficar comprometida, não apenas quando está em causa a disponibilidade física, mas também devido a qualquer outro incidente de segurança que afete a correta prestação do serviço[33].

Uma vertente de trabalho específica no âmbito do grupo de cooperação está atualmente a elaborar orientações não vinculativas em matéria de notificação sobre as circunstâncias em que os operadores de serviços essenciais são obrigados a notificar incidentes, nos termos do artigo 14.º, n.º 7, e o formato e as modalidades das notificações nacionais. As orientações deverão estar concluídas até ao quarto trimestre de 2017.

A existência de diferentes requisitos nacionais em matéria de notificação pode originar incerteza jurídica, procedimentos mais complexos e morosos e custos administrativos significativos para os operadores com atividades transfronteiras. Por conseguinte, a Comissão acolhe com agrado o trabalho do grupo de cooperação. Tal como sucede no caso dos requisitos de segurança, a Comissão incentiva os Estados-Membros a seguirem atentamente o documento de orientação a elaborar pelo grupo de cooperação, de modo a que as disposições nacionais sobre notificação de incidentes estejam, tanto quanto possível, em sintonia.

4.4. Diretiva SRI, anexo III: Prestadores de serviços digitais.

Os prestadores de serviços digitais são a segunda categoria de entidades incluídas no âmbito de aplicação da Diretiva SRI. Estas entidades são consideradas agentes económicos importantes, por serem utilizadas por muitas empresas para efeitos da prestação dos seus próprios serviços, e uma perturbação do serviço digital pode ter um impacto nas principais atividades económicas e sociais.

[33] O mesmo se aplica aos prestadores de serviços digitais.

4.4.1. Categorias de prestadores de serviços digitais.

O artigo 4.º, n.º 5, que define o serviço digital, refere-se à definição jurídica do artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535, reduzindo o âmbito de aplicação aos tipos de serviços enumerados no anexo III. Especificamente, o artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535 define estes serviços como «*qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços*» e o anexo III da Diretiva enumera três tipos de serviços específicos: mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem. Em comparação com os operadores de serviços essenciais, a diretiva não impõe aos Estados-Membros a obrigação de identificarem os prestadores de serviços digitais, que seriam depois sujeitos às obrigações relevantes. Por conseguinte, as obrigações relevantes da diretiva, nomeadamente os requisitos de segurança e de notificação estabelecidos no artigo 16.º, serão aplicáveis a todos os prestadores de serviços digitais abrangidos pelo seu âmbito de aplicação.

Os pontos que se seguem fornecem explicações complementares relativas a três tipos de serviços digitais abrangidos pelo âmbito de aplicação da diretiva.

1. Fornecedor de mercados em linha

Os mercados em linha permitem que um grande número e variedade de empresas exerçam as suas atividades comerciais em relação aos consumidores e estabeleçam relações com outras empresas. Estes mercados fornecem às empresas a infraestrutura de base para exercer o comércio em linha e além fronteiras. Desempenham um papel importante na economia, nomeadamente por proporcionarem o acesso das PME ao mercado único digital mais vasto da UE. A prestação de serviços de computação à distância que facilitam a atividade económica dos respetivos clientes, nomeadamente o processamento de transações e a agregação de dados sobre compradores, fornecedores e produtos podem também fazer parte das atividades de um fornecedor de mercados em linha, bem como a facilitação da pesquisa de produtos adequados, o fornecimento de produtos, os conhecimentos especializados em matéria de transações e a correspondência entre compradores e vendedores.

O termo mercado em linha é definido no artigo 4.º, n.º 17, e clarificado de forma mais pormenorizada no considerando 15. É descrito como um serviço que 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. Por exemplo, uma empresa como a *E-bay* pode ser considerada um fornecedor de mercado em linha, uma vez que permite a terceiros a criação de lojas na sua plataforma, a fim de que estes disponibilizem produtos e serviços por via eletrónica a consumidores ou empresas. Além disso, considera-se que as lojas de aplicações em linha para distribuição de aplicações e programas informáticos estão abrangidas pela definição de mercado em linha porque permitem que os criadores de aplicações vendam ou distribuam os respetivos serviços a consumidores ou a outras empresas. Em contrapartida, os serviços de intermediação prestados a terceiros, como o Skyscanner e os serviços de comparação de preços, que redirecionam o utilizador para o sítio do operador económico, onde é celebrado o contrato para o serviço ou produto, não são abrangidos pela definição prevista no artigo 4.º, n.º 17.

2. Fornecedor de motores de pesquisa em linha.
O termo «motor de pesquisa em linha» é definido no artigo 4.º, n.º 18, e clarificado de forma mais pormenorizada no considerando 16. É descrito como 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. Não são abrangidas as funções de pesquisa que se limitam ao conteúdo de um sítio específico ou de sítios de comparação de preços. Por exemplo, um tipo de motor de pesquisa como o oferecido pelo EUR LEX[34] não pode ser considerado um motor de pesquisa na aceção da diretiva, uma vez que a função de pesquisa se limita ao conteúdo desse sítio específico.

3. Fornecedor de serviços de computação em nuvem.
O artigo 4.º, n.º 19, define o serviço de computação em nuvem como «um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis» e o considerando 17 apresenta esclarecimentos adicionais sobre os termos «recursos computacionais», «conjunto modulável» e «adaptável».

Em resumo, a computação em nuvem pode ser descrita como um tipo específico de computação que utiliza recursos partilhados para tratar dados a pedido, sendo que os recursos partilhados se referem a qualquer tipo de componentes de equipamento ou suportes lógicos (por exemplo, redes, servidores ou outras infraestruturas, armazenamento, aplicações e serviços) que são libertados a pedido para que os utilizadores tratem dados. O termo «partilhável» define recursos de computação em que muitos utilizadores utilizam a mesma estrutura física para o tratamento de dados. O recurso de computação pode ser definido como partilhável se o conjunto de recursos utilizados pelo prestador puder ser alargado ou reduzido a qualquer momento, em função das necessidades dos utilizadores. Assim, os centros de dados ou os componentes individuais de um centro de dados podem ser eventualmente acrescentados ou retirados se a capacidade total de computação ou de armazenamento requerer uma atualização. A expressão «conjunto adaptável» pode ser descrita como as alterações do volume de trabalho mediante a disponibilização e retirada de recursos de forma automática, de modo a que, em cada momento, os recursos disponíveis correspondam o mais rigorosamente possível à procura atual[35].

Existem atualmente três tipos principais de modelos de serviço de computação em nuvem que um prestador pode oferecer:

- Infraestrutura como serviço (IaaS): categoria de serviço de computação em nuvem em que o tipo de capacidades de computação em nuvem prestadas ao cliente consiste numa infraestrutura. Inclui o fornecimento virtual de recursos de computação sob a forma de equipamento, redes e serviços de armazenamento. Servidores de alimentação, armazenamento, redes e sistemas operativos de IaaS. Fornece infraestruturas empresariais

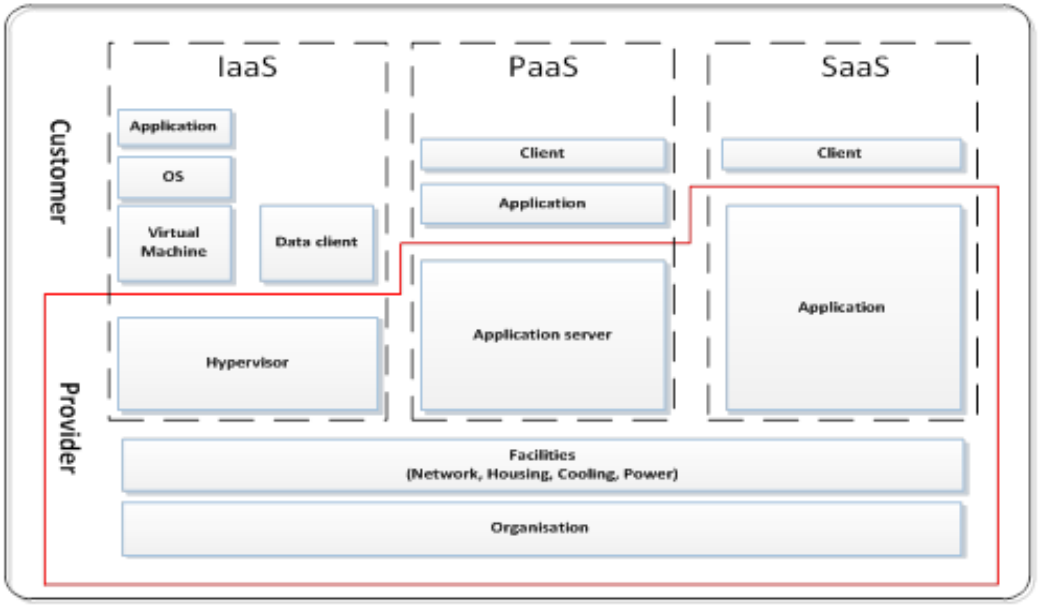
[34] Disponível em: http://eur-lex.europa.eu/homepage.html.
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, «Elasticity in Cloud Computing: What It Is, and What It Is Not», disponível em: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Ver também as páginas 2 a 5 do documento COM(2012) 529.

nas quais a empresa pode armazenar os seus dados e executar as aplicações necessárias nas suas operações quotidianas.

- Plataforma como serviço (PaaS): categoria de serviço de computação em nuvem em que o tipo de capacidades de computação em nuvem prestadas ao cliente consiste numa plataforma. Inclui plataformas de computação em linha que permitem às empresas executarem aplicações existentes ou desenvolverem e ensaiarem novas aplicações.

- Software como serviço (SaaS): categoria de serviço de computação em nuvem em que o tipo de capacidades de computação em nuvem prestadas ao cliente consiste numa aplicação ou num *software* a que se acede via Internet. Este tipo de serviços em nuvem dispensa o utilizador final da necessidade de comprar, instalar e gerir *software*, e tem a vantagem de o tornar acessível a partir de qualquer local onde haja ligação à Internet.

Figura 5: Modelos de serviço e ativos disponíveis na computação em nuvem



A ENISA forneceu orientações abrangentes sobre questões específicas no domínio da computação em nuvem[36] e um documento de orientação sobre as bases da computação em nuvem[37].

4.4.2. Requisitos de segurança.

Nos termos do artigo 16.º, n.º 1, os Estados-Membros devem assegurar que os prestadores de serviços digitais tomem as medidas técnicas e organizativas adequadas e proporcionadas para

[36] Disponível em: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Disponível em: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que as empresas utilizam na prestação dos seus serviços. Estas medidas de segurança devem ter em conta os progressos técnicos mais recentes e os cinco elementos que se seguem: i) a segurança dos sistemas e das instalações, ii) o tratamento dos incidentes, iii) a gestão da continuidade das atividades; iv) o acompanhamento, a auditoria e os testes realizados; v) a conformidade com as normas internacionais.

A este respeito, a Comissão está habilitada, nos termos do artigo 16.º, n.º 8, a adotar atos de execução que especifiquem mais pormenorizadamente esses elementos e que assegurem um elevado nível de harmonização em relação a estes prestadores de serviços. A Comissão deverá adotar o ato de execução no outono de 2017. Além disso, os Estados-Membros devem assegurar que os prestadores de serviços digitais tomem as medidas necessárias para evitar e minimizar o impacto dos incidentes, com vista a garantir a continuidade dos seus serviços.

4.4.3. Requisitos de notificação.

Os prestadores de serviços digitais devem obrigatoriamente notificar os incidentes graves às autoridades competentes ou às CSIRT. Nos termos do artigo 16.º, n.º 3, da Diretiva SRI, o requisito de notificação para os prestadores de serviços digitais aplica-se aos casos em que o incidente de segurança tem um impacto substancial na prestação do serviço. A fim de determinar esse impacto, o artigo 16.º, n.º 4, enumera em especial cinco parâmetros que devem ser tidos em conta pelos prestadores de serviços digitais. A este respeito, a Comissão está habilitada, nos termos do artigo 16.º, n.º 8, a adotar atos de execução que especifiquem mais pormenorizadamente os parâmetros. A explicação mais pormenorizada dos referidos parâmetros será parte integrante do ato de execução que especifica os elementos de segurança referidos no ponto 4.4.2, que a Comissão tenciona adotar no outono.

4.4.4. Abordagem regulamentar baseada nos riscos.

O artigo 17.º estipula que os prestadores de serviços digitais estão sujeitos a medidas de supervisão *ex post* por parte das autoridades nacionais competentes. Os Estados-Membros devem assegurar que as autoridades competentes tomem as medidas necessárias, caso lhes tenham sido apresentadas provas de que um prestador de serviços digitais não cumpre os requisitos estabelecidos no artigo 16.º da diretiva.

Além disso, nos termos do artigo 16.º, n.os 8 e 9, a Comissão está habilitada a adotar atos de execução no que diz respeito aos requisitos de notificação e de segurança, que irão reforçar o nível de harmonização no concernente aos prestadores de serviços digitais. Além disso, de acordo com o artigo 16.º, n.º 10, os Estados-Membros não podem impor quaisquer outros requisitos de segurança e de notificação aos prestadores de serviços digitais além dos estabelecidos pela diretiva, exceto nos casos em que tais medidas são necessárias para salvaguardar as funções essenciais do Estado, em particular para salvaguardar a segurança nacional, e permitir a investigação, a deteção e a ação judicial contra infrações penais.

E, por último, tendo em conta a natureza transfronteiras dos prestadores de serviços digitais, a diretiva não segue o modelo de múltiplas competências jurisdicionais paralelas, mas uma

abordagem baseada no critério do estabelecimento principal da empresa na UE.[38] Esta abordagem permite que seja aplicado um único conjunto de regras aos prestadores de serviços digitais em que uma autoridade competente é responsável pela supervisão, o que configura um aspeto particularmente importante, uma vez que muitos prestadores de serviços digitais oferecem os seus serviços em vários Estados-Membros, simultaneamente. A aplicação desta abordagem reduz ao mínimo o ónus da conformidade sobre os prestadores de serviços digitais e garante o bom funcionamento do mercado único digital.

4.4.5. Competência jurisdicional.

Tal como explicado acima, nos termos do artigo 18.º, n.º 1, da Diretiva SRI, o Estado-Membro em que o prestador de serviços digitais tem o seu estabelecimento principal tem competência jurisdicional sobre a empresa. Nos casos em que um determinado prestador de serviços digitais ofereça serviços na UE, mas não esteja estabelecido no território da UE, o artigo 18.º, n.º 2, impõe ao prestador de serviços em causa a obrigação de designar um representante na União. Nesse caso, o Estado-Membro em que o representante se encontrar estabelecido terá competência jurisdicional sobre a empresa. Nos casos em que o prestador de serviços digitais prestar serviços num Estado-Membro, mas não tiver designado um representante na UE, o Estado-Membro pode, em princípio, tomar medidas contra o prestador de serviços em causa, vez que o mesmo está a violar as suas obrigações decorrentes da diretiva.

4.4.6. Exclusão dos prestadores de serviços digitais de pequena dimensão do âmbito de aplicação dos requisitos de segurança e notificação.

Em conformidade com o artigo 16.º, n.º 11, os prestadores de serviços digitais que são microempresas ou pequenas empresas na aceção da Recomendação 2003/361/CE da Comissão39 são excluídos do âmbito de aplicação dos requisitos em matéria de segurança e notificação previstos no artigo 16.º. Assim, as empresas que empregam menos de 50 pessoas e cujo volume de negócios anual e/ou balanço anual total não exceder 10 milhões de EUR não são vinculadas por esta obrigação. Ao determinar a dimensão da entidade, não é relevante saber se a empresa em causa fornece apenas serviços digitais na aceção da Diretiva SRI ou se também presta outros serviços.

5. Relação entre a Diretiva SRI e outra legislação.

O presente ponto incide sobre as disposições relativas à *lex specialis* consagrada no artigo 1.º, n.º 7, da Diretiva SRI, ilustrando os três exemplos de *lex specialis* avaliados pela Comissão até à data, e esclarecendo quais os requisitos de segurança e notificação aplicáveis aos prestadores de serviços de telecomunicações e de serviços de confiança.

[38] Ver, nomeadamente, o artigo 18.º da diretiva.
[39] JO L 24 de 20.5.2003, p. 36.

5.1. Diretiva SRI, artigo 1.º, n.º 7: A disposição de *lex specialis.*

Nos termos do artigo 1.º, n.º 7, da Diretiva SRI, as disposições respeitantes aos requisitos de segurança e/ou de notificação relativos a prestadores de serviços digitais ou a operadores de serviços essenciais, ao abrigo da diretiva, não são aplicáveis, caso um ato jurídico setorial da UE preveja requisitos de segurança e/ou de notificação, que tenham, no mínimo, efeitos equivalentes às obrigações correspondentes da Diretiva SRI. Os Estados-Membros devem ter em conta o artigo 1.º, n.º 7, no contexto global de transposição da diretiva e fornecer informações à Comissão sobre a aplicação de disposições relativas à *lex specialis*.

Metodologia.

Ao avaliar a equivalência de um ato jurídico setorial da UE com as disposições correspondentes da Diretiva SRI, deve ser dada especial importância à questão de saber se as obrigações de segurança previstas na legislação setorial incluem medidas para garantir a segurança das redes e dos sistemas de informação, tal como definido no artigo 4.º, n.º 2, da diretiva.

No que diz respeito aos requisitos de notificação, o artigo 14.º, n.º 3, e o artigo 16.º, n.º 3, da Diretiva SRI determinam que os operadores de serviços essenciais e os prestadores de serviços digitais devem notificar as autoridades competentes ou a CSIRT, sem demora injustificada, dos incidentes com um impacto significativo ou substancial na prestação do serviço. Neste contexto, é necessário prestar especial atenção às obrigações do operador/fornecedor de serviços digitais, para incluir na notificação informações que permitam à autoridade competente ou à CSIRT determinar o eventual impacto transfronteiriço de um incidente de segurança.

Atualmente, não existe legislação setorial específica para a categoria de prestadores de serviços digitais que preveja requisitos de segurança e notificação comparáveis aos estabelecidos no artigo 16.º da Diretiva SRI e que possa ser tida em conta no contexto da aplicação do artigo 1.º, n.º 7, da Diretiva SRI[40].

No que diz respeito aos operadores de serviços essenciais, o setor financeiro e, em especial, os setores da banca e das infraestruturas do mercado financeiro, a que se referem os pontos 3 e 4 do anexo II, estão atualmente sujeitos a requisitos de segurança e/ou de notificação decorrentes de legislação setorial da União. Tal deve-se a que a segurança e a solidez das TI e das redes e sistemas de informação utilizados pelas instituições financeiras fazem parte essencial dos requisitos relativos ao risco operacional impostos às instituições financeiras por força da legislação da UE.

[40] Tal não prejudica a «Notificação de uma violação de dados pessoais à autoridade de controlo», que consta do artigo 33.º do RGPD.

Exemplos.

i) Diretiva Serviços de Pagamento 2.

No que diz respeito ao setor bancário e, em especial, à prestação de serviços de pagamento pelas instituições de crédito na aceção do artigo 4.º, n.º 1, ponto 1, do Regulamento (UE) n.º 575/2013, a denominada Diretiva Serviços de Pagamento 2 (DSP 2)[41] prevê requisitos de segurança e notificação estabelecidos nos seus artigos 95.º e 96.º.

Mais precisamente, o artigo 95.º, n.º 1, exige que os prestadores de serviços de pagamento adotem medidas de mitigação e mecanismos de controlo adequados que permitam a gestão dos riscos operacionais e de segurança relacionados com os serviços de pagamento por si prestados. Estas medidas devem incluir a criação e manutenção de procedimentos eficazes de gestão de incidentes, incluindo procedimentos para a deteção e classificação de incidentes operacionais e de segurança de caráter severo. Os considerandos 95 e 96 da DSP 2 esclarecem mais pormenorizadamente a natureza de tais medidas de segurança. De acordo com essas disposições, é evidente que as medidas previstas têm por objetivo gerir os riscos de segurança relacionados com as redes e os sistemas de informação utilizados para a prestação de serviços de pagamento. Por conseguinte, os referidos requisitos de segurança podem ser considerados, no mínimo, efeitos equivalentes à disposição correspondente do artigo 14.º, n.^{os} 1, e 2, da Diretiva SRI.

Relativamente aos requisitos de notificação, o artigo 96.º, n.º 1, da DSP 2 prevê a obrigação de os prestadores de serviços de pagamento deverem informar a autoridade competente, sem demora indevida, de incidentes de segurança de caráter severo. Além disso, comparativamente ao artigo 14.º, n.º 5, da Diretiva SRI, o artigo 96.º, n.º 2, da DPS 2, exige que a autoridade competente informe as autoridades competentes de outros Estados-Membros da relevância do incidente no seu caso. Esta obrigação implica, ao mesmo tempo, que a comunicação de incidentes de segurança tem de incluir informações que permitam às autoridades avaliar o impacto de um incidente a nível transfronteiriço. O artigo 96.º, n.º 3, alínea a), da DSP 2 confere poderes a este respeito, à EBA, em cooperação com o BCE, para emitir orientações sobre o conteúdo exato e o formato da notificação.

Por conseguinte, é possível concluir que, nos termos do artigo 1.º, n.º 7, da Diretiva SRI, tanto os requisitos de segurança como os requisitos de notificação previstos nos artigos 95.º e 96.º da DPS 2 devem aplicar-se em vez das disposições correspondentes do artigo 14.º da Diretiva SRI no que diz respeito à prestação de serviços de pagamento pelas instituições de crédito.

[41] Diretiva (UE) 2015/2366, JO L 337 de 23.12.2015, p. 35.

ii) 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.

No que diz respeito à infraestrutura do mercado financeiro, o Regulamento (UE) n.º 648/2012 em conjugação com o Regulamento (UE) n.º 153/2013 da Comissão contém disposições sobre os requisitos de segurança aplicáveis às contrapartes centrais (CCP) que podem ser consideradas *lex specialis.* Em especial, os atos jurídicos preveem medidas técnicas e organizativas relacionadas com a segurança das redes e dos sistemas de informação que, em termos de pormenor, superam os requisitos previstos no artigo 14.º, n.os 1 e 2, da Diretiva SRI, podendo, por conseguinte, considerar-se que cumprem os requisitos do artigo 1.º, n.º 7, da Diretiva SRI, no que diz respeito aos requisitos de segurança.

Mais precisamente, o artigo 26.º, n.º 1, do Regulamento (UE) n.º 648/2012 estabelece que a entidade deve dispor de «*mecanismos de governação sólidos, incluindo uma estrutura organizativa clara, com linhas de responsabilidade bem definidas, transparentes e coerentes, processos eficazes de identificação, gestão, controlo e comunicação dos riscos a que estejam ou possam vir a estar expostas e mecanismos adequados de controlo interno, nomeadamente procedimentos administrativos e contabilísticos sólidos*». O artigo 26.º, n.º 3, exige que a estrutura organizativa garanta a continuidade e o correto funcionamento dos serviços e atividades, devendo, para o efeito, pôr em prática sistemas, recursos e procedimentos adequados e proporcionados.

Além disso, o artigo 26.º, n.º 6, esclarece que as CCP devem manter «*sistemas informáticos adequados para lidar com a complexidade, variedade e tipo de serviços e atividades desenvolvidos, a fim de assegurar elevados padrões de segurança e a integridade e confidencialidade das informações que detêm*». Por outro lado, o artigo 34.º, n.º 1, impõe o estabelecimento, a aplicação e a manutenção de uma política adequada de continuidade das atividades e planos de recuperação em caso de catástrofe, destinados a garantir a recuperação atempada das operações.

Estas obrigações são especificadas de uma forma mais pormenorizada no Regulamento Delegado (UE) n.º 153/2013 da Comissão, de 19 de dezembro de 2012, que completa o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho no que diz respeito às normas técnicas de regulamentação relativas aos requisitos aplicáveis às contrapartes centrais[42]. Em especial, o artigo 4.º deste regulamento delegado impõe às CCP a obrigação de desenvolver instrumentos de gestão de riscos adequados que permitam gerir e comunicar todos os riscos pertinentes e especificar os tipos de medidas (por exemplo: a utilização de informações e sistemas de controlo de riscos sólidos, a disponibilidade de recursos, conhecimentos especializados e o acesso a todas as informações pertinentes para a unidade de gestão de riscos, a disponibilidade de mecanismos de controlo interno adequados, tais como bons procedimentos administrativos e de contabilidade para ajudar o órgão de administração

[42] JO L 52 de 23.2.2013, p. 41.

da CPP no acompanhamento e na avaliação da adequação e eficácia das suas políticas de gestão de riscos, procedimentos e sistemas).

Além disso, o artigo 9.º refere expressamente a segurança dos sistemas de tecnologias da informação, e impõe a adoção de medidas técnicas e organizativas específicas relacionadas com a manutenção de um quadro sólido de segurança da informação para a gestão dos riscos em matéria de segurança informática. Essas medidas devem incluir mecanismos e procedimentos que garantam a disponibilidade dos serviços, bem como a proteção da autenticidade, integridade e confidencialidade dos dados.

iii) 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[43].

No que diz respeito às plataformas de negociação, o artigo 48.º, n.º 1, da Diretiva 2014/65/UE exige que os operadores garantam a continuidade dos seus serviços em caso de qualquer falha dos seus sistemas de negociação. Esta obrigação geral foi recentemente especificada e completada pelo Regulamento Delegado (UE) 2017/584 da Comissão,[44] de 14 de julho de 2016, que complementa a Diretiva 2014/65/UE do Parlamento Europeu e do Conselho no que diz respeito às normas técnicas de regulamentação que especificam os requisitos em matéria de organização das plataformas de negociação[45]. Em especial, o artigo 23.º, n.º 1, deste regulamento estipula que as plataformas de negociação devem dispor de procedimentos e disposições em matéria de segurança física e eletrónica destinados a proteger os seus sistemas contra a utilização indevida ou o acesso não autorizado e a assegurar a integridade dos dados. Estas medidas devem permitir a prevenção ou minimização dos riscos de ataques contra os sistemas de informação.

O artigo 23.º, n.º 2, exige ainda que as medidas e as disposições tomadas pelos operadores devam permitir a rápida identificação e gestão dos riscos relacionados com qualquer acesso não autorizado, interferências no sistema que prejudiquem gravemente ou interrompam o funcionamento de sistemas de informação e interferências em dados que comprometam a sua disponibilidade, integridade ou autenticidade. Além disso, o artigo 15.º do Regulamento impõe a obrigação de as plataformas de negociação disporem de planos de continuidade das atividades eficazes para assegurar a estabilidade suficiente do sistema e fazer face a incidentes que provoquem perturbações. Em especial, estas medidas devem permitir que o operador retome a negociação no prazo de duas horas e, ao mesmo tempo, garantir que a quantidade de dados perdidos é próxima de zero.

O artigo 16.º determina ainda que as medidas identificadas para dar resposta e gerir incidentes causadores de perturbações devem fazer parte do plano de continuidade das atividades das plataformas de negociação e prevê elementos específicos que devem ser tidos em conta pelo

[43] JO L 173 de 12.6.2014, p. 349.
[44] JO L 87 de 31.3.2017, p. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf.

operador aquando da adoção do plano de continuidade das atividades (por exemplo, a criação de uma equipa específica de operações de segurança, a realização de uma avaliação de impacto para identificar os riscos que seja periodicamente revista).

Tendo em conta o conteúdo das medidas de segurança referidas, afigura-se que se destinam a gerir e enfrentar os riscos associados à disponibilidade, autenticidade, integridade e confidencialidade dos dados ou serviços prestados e, por conseguinte, pode concluir-se que a legislação setorial da UE anteriormente referida contém obrigações de segurança que são, pelo menos, equivalentes às obrigações correspondentes previstas no artigo 14.º, n.os 1 e 2, da Diretiva SRI.

5.2 Diretiva SRI, artigo 1.º, n.º 3: Prestadores de serviços de telecomunicações e prestadores de serviços de confiança.

Nos termos do artigo 1.º, n.º 3, os requisitos de segurança e notificação previstos na diretiva não são aplicáveis aos prestadores de serviços que estejam sujeitos aos requisitos previstos nos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE. Os artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE aplicam-se às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público. Por conseguinte, no que se refere ao fornecimento de redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, a empresa tem de cumprir os requisitos de segurança e de notificação previstos na Diretiva 2002/21/CE.

No entanto, se a mesma empresa presta também outros serviços, como serviços digitais (p. ex.: computação em nuvem ou mercado em linha) enumerados no anexo III da Diretiva SRI, ou serviços como o DNS ou pontos de troca de tráfego, nos termos do anexo II, ponto 7, da Diretiva SRI, a empresa ficará sujeita aos requisitos de segurança e notificação previstos na Diretiva SRI no tocante à prestação desses serviços específicos. Importa salientar que, por os prestadores de serviços referidos no anexo II, ponto 7, pertencerem à categoria de operadores de serviços essenciais, os Estados-Membros são obrigados a realizar um processo de identificação, nos termos do artigo 5.º, n.º 2, e determinar quais os prestadores individuais de serviços de DNS, de pontos de troca de tráfego ou de TLD que devem cumprir os requisitos da Diretiva SRI. Isto significa que, na sequência dessa apreciação, apenas os prestadores de DNS, pontos de troca de tráfego ou TLD que preencham os critérios previstos no artigo 5.º, n.º 2, da Diretiva SRI estão sujeitos à obrigação de cumprimento dos requisitos previstos na Diretiva SRI.

O artigo 1.º, n.º 3, especifica igualmente que os requisitos de segurança e de notificação previstos na diretiva também não são aplicáveis aos prestadores de serviços de confiança que estejam sujeitos a requisitos semelhantes nos termos do artigo 19.º do Regulamento (UE) n.º 910/2014.

6. Documentos publicados sobre estratégias nacionais de cibersegurança.

	Estado-Membro	Título da estratégia e ligações disponíveis
1	Áustria	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Bélgica	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgária	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Croácia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	República Checa	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Chipre	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Dinamarca	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estónia	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finlândia	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	França	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irlanda	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Itália	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Alemanha	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Hungria	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Letónia	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lituânia	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxemburgo	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Países Baixos	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polónia	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Roménia	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	República Eslovaca	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Eslovénia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Espanha	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Suécia	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Reino Unido	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Lista de boas práticas e recomendações emitidas pela ENISA.

Em relação à resposta a incidentes

- ✓ Estratégias de resposta a incidentes e cooperação em caso de cibercrises[46]

Em relação ao tratamento de incidentes

- ✓ Projeto de automatização do tratamento de incidentes[47]
- ✓ Guia de boas práticas para a gestão de incidentes[48]

Em relação à classificação e taxonomia dos incidentes

- ✓ Síntese das atuais taxonomias[49]
- ✓ Guia de boas práticas para a utilização de taxonomias na prevenção e deteção de incidentes[50]

Em relação à maturidade das CSIRT

- ✓ Desafios para as CSIRT nacionais na Europa em 2016: Estudo sobre a maturidade das CSIRT[51]
- ✓ Estudo sobre a maturidade das CSIRT — Processo de avaliação[52]
- ✓ Orientações para as CSIRT nacionais e governamentais sobre a forma de avaliar a maturidade[53]

Em relação ao reforço das capacidades e à formação das CSIRT

- ✓ Guia de boas práticas sobre metodologias de formação[54]

Para mais informações sobre as CSIRT existentes na Europa ─ Visão geral das CSIRT por país[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Disponível em: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.
[47] Mais informações em: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Disponível em: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.
[49] Mais informações em: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Disponível em: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection.
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Disponível em: https://www.enisa.europa.eu/publications/study-on-csirt-maturity.
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Disponível em: https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Disponível em: https://www.enisa.europa.eu/publications/csirt-capabilities.
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Disponível em: https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.
[55] Mais informações em: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.