Conselho da
União Europeia

Bruxelas, 16 de setembro de 2022
(OR. en)

12429/22

Dossiê interinstitucional:
2022/0272 (COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PROPOSTA

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	15 de setembro de 2022
para:	Secretariado-Geral do Conselho
n.° doc. Com.:	COM(2022) 454 final
Assunto:	Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 454 final.

Anexo: COM(2022) 454 final

COMISSÃO
EUROPEIA

Bruxelas, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

(Texto relevante para efeitos do EEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

Os produtos de *hardware* e *software* estão cada vez mais sujeitos a ciberataques bem-sucedidos, o que terá dado origem a um custo anual global estimado da cibercriminalidade de 5,5 biliões de EUR até 2021. Estes produtos são afetados por dois problemas importantes que aumentam os custos para os utilizadores e para a sociedade: 1) um baixo nível de cibersegurança, que se traduz em vulnerabilidades generalizadas e numa disponibilização insuficiente e incoerente de atualizações de segurança para as resolver, e 2) um entendimento e um acesso deficientes dos utilizadores à informação, o que os impede de escolher produtos com propriedades de cibersegurança adequadas ou de os utilizar de forma segura. Num ambiente conectado, um incidente de cibersegurança num produto pode afetar toda uma organização ou toda a cadeia de abastecimento, propagando-se muitas vezes através das fronteiras do mercado interno numa questão de minutos, o que pode provocar perturbações graves das atividades económicas e sociais ou mesmo tornar-se uma ameaça para a vida das pessoas.

A cibersegurança dos produtos com elementos digitais tem uma forte dimensão transfronteiriça, uma vez que os produtos fabricados num país são muitas vezes utilizados em todo o mercado interno. Além disso, os incidentes que afetam inicialmente uma única entidade ou um único Estado-Membro propagam-se com frequência numa questão de minutos por todo o mercado interno.

Embora a legislação em vigor relativa ao mercado interno se aplique a determinados produtos com elementos digitais, a maioria dos produtos de *hardware* e *software* não está atualmente abrangida por nenhuma legislação da UE que aborde a sua cibersegurança. Em especial, o atual quadro jurídico da UE não aborda a cibersegurança de *software* não incorporado, apesar de os ataques de cibersegurança visarem cada vez mais as vulnerabilidades destes produtos, dando origem a custos sociais e económicos significativos. Existem numerosos exemplos de ciberataques importantes, resultantes de uma segurança insuficiente dos produtos, como o *software* de sequestro (do tipo verme) WannaCry, que explorou uma vulnerabilidade do Windows que afetou, em 2017, 200 000 computadores em 150 países e causou danos no montante de milhares de milhões de USD; o ataque à cadeia de abastecimento do Kaseya VSA, que utilizou o *software* de administração da rede da Kaseya para atacar mais de 1 000 empresas e forçou uma cadeia de supermercados a encerrar as suas 500 lojas em toda a Suécia; ou os inúmeros incidentes em que aplicações bancárias são pirateadas para roubar dinheiro a consumidores incautos.

Foram identificados dois objetivos principais destinados a assegurar o bom funcionamento do mercado interno: 1) criar condições para o desenvolvimento de produtos com elementos digitais seguros, assegurando que sejam colocados no mercado produtos de *hardware* e *software* com menos vulnerabilidades, e garantir que os fabricantes encarem a segurança com seriedade ao longo de todo o ciclo de vida de um produto; e 2) criar condições que permitam aos utilizadores ter em conta a cibersegurança aquando da seleção e da utilização de produtos com elementos digitais. Foram definidos quatro objetivos específicos: i) assegurar que os fabricantes melhorem a segurança dos produtos com elementos digitais desde a fase de conceção e desenvolvimento e ao longo de todo o ciclo de vida; ii) assegurar um quadro de cibersegurança coerente, que facilite a conformidade por parte dos produtores de *hardware* e *software*; iii) aumentar a transparência das propriedades de segurança dos produtos com elementos digitais; e iv) permitir que as empresas e os consumidores utilizem produtos com elementos digitais de forma segura.

A natureza marcadamente transfronteiriça da cibersegurança e o aumento dos incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada. Dada a natureza global dos mercados de produtos com elementos digitais, os Estados-Membros enfrentam, no respetivo território, os mesmos riscos para o mesmo produto com elementos digitais. Um quadro fragmentado emergente de regras nacionais potencialmente divergentes pode prejudicar um mercado único aberto e competitivo para os produtos com elementos digitais. Torna-se, deste modo, necessária uma ação conjunta a nível da UE a fim de aumentar o nível de confiança entre os utilizadores e a atratividade dos produtos da UE com elementos digitais. Esta beneficiará igualmente o mercado interno, proporcionando segurança jurídica e criando condições de concorrência equitativas para os vendedores de produtos com elementos digitais, conforme salientado no relatório final da Conferência sobre o Futuro da Europa, em que os cidadãos apelam ao reforço do papel da UE na luta contra as ameaças à cibersegurança.

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

O quadro da UE inclui vários atos legislativos horizontais que abrangem determinados aspetos relacionados com a cibersegurança a partir de diferentes ângulos (produtos, serviços, gestão de crises e crimes). Em 2013, entrou em vigor a Diretiva relativa a ataques contra os sistemas de informação[1], que harmoniza a criminalização e as sanções aplicáveis a um conjunto de infrações contra os sistemas de informação. Em agosto de 2016, entrou em vigor a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação (Diretiva SRI)[2]. Trata-se do primeiro ato legislativo a nível da UE em matéria de cibersegurança. A sua revisão, que resultou na Diretiva [Diretiva XXX/XXXX (SRI 2)], aumenta o nível comum de ambição da UE. Em 2019, entrou em vigor o Regulamento Cibersegurança[3] destinado a reforçar a segurança dos produtos, serviços e processos de TIC através da introdução de um quadro europeu para a certificação voluntária da cibersegurança[4].

Só é possível garantir a cibersegurança de toda a cadeia de abastecimento se a totalidade dos seus componentes estiver protegida contra as ciberameaças. No entanto, a legislação da UE acima referida apresenta lacunas a este respeito, uma vez que não abrange os requisitos obrigatórios para a segurança dos produtos com elementos digitais.

Se a proposta de ato legislativo sobre a ciber-resiliência abrange produtos com elementos digitais colocados no mercado, a Diretiva [Diretiva XXX/XXX (SRI 2)] visa assegurar um elevado nível de cibersegurança dos serviços prestados por entidades essenciais e importantes. A Diretiva [Diretiva XXX/XXXX (SRI 2)] exige que os Estados-Membros assegurem que as entidades essenciais e importantes abrangidas pelo âmbito de aplicação, como os prestadores de cuidados de saúde ou de serviços de computação em nuvem e as entidades da administração pública, tomem medidas técnicas, operacionais e organizativas adequadas e proporcionadas em matéria de cibersegurança. Tal inclui, nomeadamente, um requisito para

---

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

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

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

4 O Regulamento Cibersegurança permite o desenvolvimento de sistemas de certificação específicos. Cada sistema inclui referências a normas, especificações técnicas ou outros requisitos de cibersegurança pertinentes definidos no sistema. A decisão de elaborar uma certificação da cibersegurança baseia-se no risco.

garantir a segurança na aquisição, desenvolvimento e manutenção das redes e dos sistemas de informação, incluindo o tratamento e a divulgação de vulnerabilidades. A Diretiva [Diretiva XXX/XXXX (SRI 2)] exige que a Comissão adote atos de execução que estabeleçam os requisitos técnicos e metodológicos dessas medidas no prazo de 21 meses a contar da data de entrada em vigor desta diretiva para determinados tipos de entidades, como os prestadores de serviços de computação em nuvem. No caso das demais entidades, a Comissão pode adotar um ato de execução que estabeleça os requisitos técnicos e metodológicos, bem como os requisitos setoriais. Este quadro assegurará que as especificações técnicas e as medidas semelhantes aos requisitos essenciais de cibersegurança do ato legislativo sobre a ciber-resiliência também sejam aplicadas para a conceção, o desenvolvimento e o tratamento das vulnerabilidades do *software* prestado como um serviço (*software-as-a-service*). Tal poderá, por exemplo, constituir um meio para assegurar um elevado nível de cibersegurança em casos como os sistemas de registos de saúde eletrónicos (RSE), nomeadamente quando fornecidos sob a forma de *software* como serviço (SaaS) ou desenvolvidos em instituições de saúde (internamente), em conformidade com a proposta de [Regulamento Espaço Europeu de Dados de Saúde].

- **Interação com outras políticas da União**

Tal como referido na Comunicação «Construir o futuro digital da Europa»[5], é crucial que a UE tire partido de todos os benefícios da era digital e reforce a sua capacidade industrial e de inovação dentro de limites éticos e seguros. A estratégia europeia para os dados define quatro pilares – a proteção de dados, os direitos fundamentais, a segurança e a cibersegurança –, que constituem condições essenciais para uma sociedade capacitada pela utilização dos dados.

O quadro jurídico da UE[6] atualmente aplicável aos produtos que possam conter elementos digitais inclui vários atos legislativos, como a legislação da UE sobre produtos específicos respeitante aos aspetos ligados à segurança e a legislação geral em matéria de responsabilidade pelos produtos. A proposta é coerente com o atual quadro regulamentar da UE relacionado com os produtos, assim como com as recentes propostas legislativas, como a proposta de regulamento da Comissão [Regulamento Inteligência Artificial (IA)][7].

A proposta de regulamento será aplicável a todos os equipamentos de rádio no âmbito de aplicação do Regulamento Delegado (UE) 2022/30 da Comissão. Além disso, os requisitos estabelecidos no presente regulamento incluem todos os elementos dos requisitos essenciais a que se refere o artigo 3.º, n.º 3, alíneas d), e) e f), da Diretiva 2014/53/UE, incluindo os principais elementos estabelecidos na [Decisão de Execução XXX/2022 da Comissão relativa a um pedido de normalização às organizações europeias de normalização] emitido com base nesse regulamento delegado. A fim de evitar uma sobreposição regulamentar, prevê-se que a Comissão revogue ou altere o regulamento delegado no que diz respeito aos equipamentos de rádio abrangidos pelo regulamento proposto, de modo que este último lhes seja aplicável, assim que entrar em vigor.

Além disso, a fim de evitar uma duplicação de esforços, prevê-se que a Comissão e as organizações europeias de normalização tenham em conta o trabalho de normalização realizado no contexto da Decisão de Execução C(2022)5637 da Comissão relativa a um

---

5 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Construir o futuro digital da Europa», de 19 de fevereiro de 2020 [COM(2020) 67 final].

6 Principalmente a legislação relativa ao novo quadro legislativo (NQL).

7 Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, de 21 de abril de 2021 [COM(2021) 206 final].

pedido de normalização para o Regulamento Delegado 2022/30 da DER na elaboração e desenvolvimento de normas harmonizadas para facilitar a aplicação do regulamento.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

A base jurídica da proposta é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que prevê a adoção de medidas para assegurar o estabelecimento e o funcionamento do mercado interno. O objetivo da proposta é harmonizar os requisitos de cibersegurança dos produtos com elementos digitais em todos os Estados-Membros e eliminar os obstáculos à livre circulação de mercadorias.

O artigo 114.º do TFUE pode ser utilizado como base jurídica para evitar a ocorrência destes obstáculos resultantes de leis e abordagens nacionais divergentes sobre a forma de resolver as incertezas e as lacunas jurídicas nos quadros jurídicos existentes[8]. Além disso, o Tribunal de Justiça reconheceu que a aplicação de requisitos técnicos heterogéneos pode constituir um motivo válido para desencadear a aplicação do artigo 114.º do TFUE[9].

O atual quadro legislativo da UE aplicável aos produtos com elementos digitais baseia-se no artigo 114.º do TFUE e compreende vários atos legislativos, incluindo sobre produtos específicos e aspetos ligados à segurança ou a legislação geral em matéria de responsabilidade pelos produtos. No entanto, abrange apenas determinados aspetos relacionados com a cibersegurança de produtos digitais corpóreos e, se for caso disso, de *software* incorporado nesses produtos. A nível nacional, os Estados-Membros começam a tomar medidas nacionais que exigem que os fornecedores de produtos digitais reforcem a sua cibersegurança[10]. Paralelamente, a cibersegurança dos produtos digitais tem uma dimensão transfronteiriça particularmente forte, uma vez que os produtos fabricados num país são muitas vezes utilizados por organizações e consumidores em todo o mercado interno. Os incidentes que inicialmente dizem respeito a uma só entidade ou Estado-Membro propagam-se com frequência numa questão de minutos por organizações, setores e vários Estados-Membros.

Os vários atos e iniciativas adotados até à data a nível da UE e a nível nacional apenas abordam parcialmente os problemas identificados e correm o risco de criar um mosaico legislativo no mercado interno, aumentando a insegurança jurídica tanto para os fornecedores como para os utilizadores destes produtos e impondo desnecessariamente mais encargos às empresas no cumprimento de uma série de requisitos para tipos semelhantes de produtos.

O regulamento proposto harmonizará e simplificará o quadro regulamentar da UE, introduzindo requisitos de cibersegurança dos produtos com elementos digitais e evitando a sobreposição de requisitos decorrentes de diferentes atos legislativos. Criar-se-á, assim, uma maior segurança jurídica para os operadores e utilizadores em toda a União, bem como uma melhor harmonização do mercado único europeu, dando origem a condições mais viáveis para os operadores que pretendam entrar no mercado da UE.

---

8 Acórdão do Tribunal de Justiça (Grande Secção) de 3 de dezembro de 2019 no processo C-482/17, República Checa/Parlamento Europeu e Conselho da União Europeia, n.º 35.

9 Acórdão do Tribunal de Justiça (Grande Secção) de 2 de maio de 2006 no processo C-217/04, Reino Unido da Grã-Bretanha e da Irlanda do Norte/Parlamento Europeu e Conselho da União Europeia, n.os 62-63.

10 Em 2019, por exemplo, a Finlândia criou um sistema de rotulagem para os dispositivos da IdC, como televisores inteligentes, telemóveis inteligentes e brinquedos, com base nas normas do ETSI. A Alemanha introduziu recentemente um rótulo de segurança dos consumidores para encaminhadores de banda larga, televisores inteligentes, câmaras, altifalantes, brinquedos, bem como robôs de limpeza e jardinagem.

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

A natureza marcadamente transfronteiriça da cibersegurança em geral e o número crescente de riscos e incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos da presente intervenção não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada. As abordagens nacionais à resolução dos problemas e, em especial, as abordagens que introduzem requisitos obrigatórios criarão insegurança jurídica e barreiras jurídicas adicionais. As empresas poderão deparar-se com obstáculos à sua fácil expansão para outros Estados-Membros, privando os utilizadores dos benefícios dos seus produtos.

Por conseguinte, é necessária uma ação conjunta a nível da UE para estabelecer um elevado nível de confiança entre os utilizadores, aumentando a atratividade dos produtos da UE com elementos digitais. Esta beneficiará igualmente o mercado único digital e o mercado interno em geral, proporcionando segurança jurídica e criando condições de concorrência equitativas para os fabricantes de produtos com elementos digitais.

Em última análise, as Conclusões do Conselho de 23 de maio de 2022 sobre o desenvolvimento da postura da União Europeia no ciberespaço instam a Comissão a propor, até ao final de 2022, requisitos comuns de cibersegurança para os dispositivos conectados.

- **Proporcionalidade**

No que diz respeito à proporcionalidade do regulamento proposto, as medidas previstas nas opções estratégicas consideradas não excederão o necessário para alcançar os objetivos gerais e específicos e não implicarão custos desproporcionados. Mais concretamente, a intervenção considerada assegurará a proteção dos produtos com elementos digitais ao longo de todo o seu ciclo de vida e proporcionalmente aos riscos enfrentados através de requisitos orientados para objetivos e neutros do ponto de vista tecnológico, que continuam a ser razoáveis e correspondem, de modo geral, ao interesse das entidades envolvidas.

Os requisitos essenciais de cibersegurança da proposta baseiam-se em normas amplamente utilizadas e o processo de normalização subsequente terá em conta as especificidades técnicas dos produtos. Quer isto dizer que, sempre que necessário para um determinado nível de risco, os controlos de segurança serão adaptados. Além disso, as regras horizontais previstas apenas contemplarão a avaliação por terceiros de produtos críticos, o que incluirá apenas uma parte limitada do mercado de produtos com elementos digitais. O impacto nas PME dependerá da sua presença no mercado destas categorias específicas de produtos.

No que se refere à proporcionalidade dos custos da avaliação da conformidade, os organismos notificados que realizam as avaliações externas terão em conta a dimensão da empresa ao fixarem as taxas. Será igualmente previsto um período de transição razoável de 24 meses para preparar a execução, o que dá tempo aos mercados relevantes para se prepararem, transmitindo simultaneamente uma orientação clara para os investimentos em I&D. Quaisquer custos de conformidade para as empresas serão compensados pelos benefícios proporcionados por um nível mais elevado de segurança dos produtos com elementos digitais e, em última análise, pelo aumento da confiança dos utilizadores nestes produtos.

- **Escolha do instrumento**

Uma intervenção regulamentar implicará a adoção de um regulamento e não de uma diretiva. Com efeito, para este tipo específico de legislação relativa a produtos, um regulamento resolverá de forma mais eficaz os problemas identificados e cumprirá os objetivos formulados, uma vez que se trata de uma intervenção que condiciona a colocação no mercado interno de uma categoria muito vasta de produtos. O processo de transposição, no caso de uma diretiva relativa a esse tipo de intervenção, poderá deixar uma margem discricionária excessiva a nível nacional, conduzindo potencialmente à falta de uniformidade de certos requisitos essenciais em matéria de cibersegurança, à insegurança jurídica, a uma maior

fragmentação ou mesmo a situações discriminatórias transfronteiriças, tanto mais se for tido em conta o facto de os produtos abrangidos poderem ter múltiplas finalidades ou utilizações e de os fabricantes poderem produzir várias categorias desses produtos.

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

- **Consultas das partes interessadas**

A Comissão consultou um vasto leque de partes interessadas. Os Estados-Membros e as partes interessadas foram convidados a participar na consulta pública aberta e nos inquéritos e seminários organizados no contexto de um estudo de apoio aos trabalhos preparatórios da Comissão para a avaliação de impacto realizado por um consórcio composto pela Wavestone, pelo Centro de Estudos de Política Europeia (CEPE) e pela ICF. As partes interessadas consultadas incluíram autoridades nacionais de fiscalização do mercado, organismos da União que lidam com a cibersegurança, fabricantes de *hardware* e *software*, importadores e distribuidores de *hardware* e *software*, associações comerciais, organizações de consumidores e utilizadores de produtos com elementos digitais e cidadãos, investigadores e universidades, organismos notificados e organismos de acreditação e ainda profissionais do setor da cibersegurança.

As atividades de consulta incluíram:

- Um primeiro estudo realizado por um consórcio composto pela ICF, a Wavestone, a Carsa e o CEPE, que foi publicado em dezembro de 2021[11]. O estudo identificou várias deficiências do mercado e avaliou possíveis intervenções regulamentares.
- Uma consulta pública aberta dirigida a cidadãos, partes interessadas e peritos em cibersegurança. Foram apresentadas 176 respostas. Estas contribuíram para a recolha de opiniões e experiências diversas de todos os grupos de partes interessadas.
- Os seminários organizados no âmbito do estudo de apoio aos trabalhos preparatórios da Comissão para um ato legislativo sobre a ciber-resiliência reuniram cerca de 100 representantes de uma série de partes interessadas, provenientes dos 27 Estados-Membros.
- Foram realizadas entrevistas a especialistas para obter um entendimento mais aprofundado dos atuais desafios em matéria de cibersegurança relacionados com produtos com elementos digitais, bem como para debater opções estratégicas para uma eventual intervenção regulamentar.
- Foram realizados debates bilaterais com as autoridades nacionais de cibersegurança, o setor privado e as organizações de consumidores.
- Foram conduzidas ações de sensibilização específicas junto das principais partes interessadas das PME.

- **Recolha e utilização de conhecimentos especializados**

As atividades de consulta visaram obter contributos sobre os cinco principais critérios de avaliação com base nas orientações da UE para legislar melhor (eficácia, eficiência,

[11] *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715, Final Study Report* (não traduzido para português), disponível em https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

pertinência, coerência, valor acrescentado da UE), assim como sobre os potenciais impactos de possíveis opções para o futuro. O contratante não só contactou as partes interessadas que serão diretamente afetadas pela proposta de regulamento, como também consultou um vasto leque de peritos no domínio da cibersegurança.

- **Avaliação de impacto**

A Comissão realizou uma avaliação de impacto da presente proposta, que foi analisada pelo Comité de Controlo da Regulamentação (CCR) da Comissão. Em 6 de julho de 2022, realizou-se uma reunião com o CCR, a que se seguiu um parecer positivo. A avaliação de impacto foi ajustada para dar resposta às recomendações e observações do CCR.

A Comissão examinou diferentes opções estratégicas para alcançar os objetivos gerais da proposta:

- Abordagem não vinculativa e medidas voluntárias (opção 1): nesta opção, não haveria qualquer intervenção regulamentar obrigatória. Pelo contrário, a Comissão emitiria comunicações, orientações, recomendações e, eventualmente, códigos de conduta para incentivar medidas voluntárias. Continuariam a ser desenvolvidos regimes nacionais, voluntários ou obrigatórios, a fim de compensar a ausência de regras horizontais da UE.
- Intervenção regulamentar *ad hoc* específica para a cibersegurança dos produtos corpóreos com elementos digitais e respetivo *software* incorporado (opção 2): esta opção implicaria uma intervenção regulamentar *ad hoc* específica para cada produto, que se limitaria a acrescentar e/ou a alterar os requisitos de cibersegurança na legislação já em vigor ou a introduzir nova legislação à medida que surgissem novos riscos, incluindo, eventualmente, sobre *software* não incorporado.

As opções 3 e 4 implicam uma intervenção regulamentar horizontal de âmbito variável, em grande medida em conformidade com o novo quadro legislativo (NQL). Este quadro estabelece requisitos essenciais como condição para a colocação de determinados produtos no mercado interno. O NQL também prevê, por norma, uma avaliação da conformidade, um processo conduzido pelo fabricante para demonstrar se foram cumpridos os requisitos especificados relativos a um produto.

- Abordagem mista, incluindo regras vinculativas horizontais sobre a cibersegurança dos produtos corpóreos com elementos digitais e respetivo *software* incorporado e uma abordagem faseada para o *software* não incorporado (opção 3): esta opção implicaria um regulamento que introduz requisitos horizontais de cibersegurança para todos os produtos corpóreos com elementos digitais e o *software* neles incorporado, como condição para a colocação no mercado, e incluiria duas subopções com e sem avaliação obrigatória por terceiros (3i e 3ii). O *software* não incorporado não seria regulamentado.
- Uma intervenção regulamentar horizontal que introduz requisitos de cibersegurança para uma vasta gama de produtos digitais corpóreos e não corpóreos com elementos digitais, incluindo *software* não incorporado (opção 4): esta opção assemelha-se à opção 3, com exceção do âmbito de aplicação. A opção 4 incluiria o *software* não incorporado (com duas subopções que englobariam, respetivamente, apenas o *software* crítico (4a) ou todo o *software* (4a) no âmbito de um eventual regulamento. Para cada subopção, seriam consideradas as mesmas subopções relacionadas com a avaliação da conformidade que para a opção 3.

A opção 4 (com subopções que abrangem todo o *software* e envolvem a avaliação obrigatória por terceiros de produtos críticos) foi considerada a opção preferida com base na avaliação da eficácia em relação aos objetivos específicos e à eficiência custos-benefícios. Esta opção assegurará a definição de requisitos horizontais específicos de cibersegurança para todos os produtos com elementos digitais colocados ou disponibilizados no mercado interno e será a única opção a abranger toda a cadeia de abastecimento digital. O *software* não incorporado, muitas vezes exposto a vulnerabilidades, também será abrangido por essa intervenção regulamentar, assegurando assim uma abordagem coerente em relação a todos os produtos com elementos digitais, com uma partilha clara das responsabilidades dos vários operadores económicos.

Esta opção estratégica também proporciona valor acrescentado ao abranger aspetos relacionados com o dever de diligência e todo o ciclo de vida após a colocação dos produtos com elementos digitais no mercado, a fim de assegurar, nomeadamente, informações adequadas sobre o apoio prestado no domínio da segurança e a disponibilização de atualizações de segurança. Esta opção estratégica será também mais eficaz para complementar a recente revisão do quadro de SRI, garantindo os pré-requisitos para uma segurança reforçada da cadeia de abastecimento.

A opção preferida gerará benefícios significativos para as várias partes interessadas. Para as empresas, permitirá evitar a aplicação de regras de segurança divergentes aos produtos com elementos digitais e reduzir os custos de conformidade com a legislação conexa em matéria de cibersegurança. Reduzirá o número de ciberincidentes, os custos do tratamento de incidentes e os danos à reputação. Para a UE no seu conjunto, estima-se que a iniciativa possa conduzir a uma redução dos custos decorrentes de incidentes que afetam as empresas em cerca de 180 a 290 mil milhões de EUR por ano. Conduzirá a um aumento do volume de negócios em virtude do aumento da procura de produtos com elementos digitais. Melhorará a reputação global das empresas, levando a um aumento da procura também por parte de países terceiros. Para os utilizadores, a opção preferida reforçará a transparência das propriedades de segurança e facilitará a utilização de produtos com elementos digitais. Os consumidores e os cidadãos também beneficiarão de uma melhor proteção dos seus direitos fundamentais, como a privacidade e a proteção de dados.

Quando convidados a classificar a eficácia das intervenções estratégicas, os respondentes na consulta pública concordaram que a opção 4 seria a medida mais eficaz (4,08 numa escala de 1 a 5). Entre os respondentes, contavam-se organizações de consumidores (5,00), pessoas que se identificavam como utilizadores (4,22), organismos notificados (4,17), autoridades de fiscalização do mercado (5,00) e produtores de produtos com elementos digitais (3,85), incluindo os de pequena e média dimensão (4,05).

- **Adequação da regulamentação e simplificação**

A presente proposta estabelece requisitos aplicáveis aos fabricantes de *software* e *hardware*. Verifica-se a necessidade de garantir a segurança jurídica e evitar uma maior fragmentação, a nível do mercado, dos requisitos de cibersegurança relacionados com os produtos no mercado interno, o que foi demonstrado pelo amplo apoio de várias partes interessadas a uma intervenção horizontal. A proposta minimizará os encargos regulamentares impostos aos fabricantes por vários atos legislativos em matéria de segurança dos produtos. O alinhamento com o NQL significa um melhor funcionamento da intervenção e da sua aplicação. A proposta simplifica o processo dos procedimentos de salvaguarda ao envolver os fabricantes e os Estados-Membros de a Comissão ser notificada. Uma grande parte dos fabricantes abrangidos pelo âmbito de aplicação da proposta já está familiarizada com o funcionamento do NQL, o que contribuirá para a sua compreensão e aplicação. Para os consumidores e as empresas, a proposta promoverá a confiança nos produtos com elementos digitais.

- **Direitos fundamentais**

Espera-se que todas as opções estratégicas reforcem, em certa medida, a proteção dos direitos e liberdades fundamentais, como a privacidade, a proteção dos dados pessoais, a liberdade de empresa e a proteção da propriedade ou da dignidade e integridade pessoais. Em especial, a opção 4 (a opção preferida), que consiste em intervenções regulamentares horizontais e num vasto âmbito político, será a mais eficaz a este respeito, uma vez que é mais provável que ajude a reduzir o número e a gravidade dos incidentes, incluindo as violações de dados pessoais. Aumentará igualmente a segurança jurídica e assegurará condições equitativas para os operadores económicos, reforçará a confiança entre os utilizadores e a atratividade dos produtos da UE com elementos digitais no seu conjunto, protegendo assim a propriedade e melhorando as condições para os operadores económicos exercerem a sua atividade.

Os requisitos horizontais de cibersegurança contribuirão para a segurança dos dados pessoais, protegendo a confidencialidade, a integridade e a disponibilidade de informações em produtos com elementos digitais. O cumprimento desses requisitos facilitará o cumprimento do requisito de segurança do tratamento de dados pessoais previsto no Regulamento (UE) 2016/679 relativo à proteção de dados (RGPD)[12]. A proposta reforçará a transparência e a informação dos utilizadores, incluindo aqueles que possam possuir menos competências em matéria de cibersegurança. Os utilizadores estarão também mais bem informados sobre os riscos, as capacidades e as limitações dos produtos com elementos digitais, o que os colocará numa melhor posição para tomar as medidas preventivas e de atenuação necessárias para reduzir os riscos residuais.

4. INCIDÊNCIA ORÇAMENTAL

A fim de desempenhar as funções atribuídas à Agência da União Europeia para a Cibersegurança (ENISA) ao abrigo do presente regulamento, a ENISA terá de reafetar recursos na ordem dos 4,5 ETC aproximadamente. A Comissão terá de atribuir 7 ETC para cumprir as suas responsabilidades em matéria de execução ao abrigo do presente regulamento.

É disponibilizada uma panorâmica pormenorizada dos custos na «ficha financeira» anexa à presente proposta.

5. OUTROS ELEMENTOS

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

A Comissão acompanhará a execução, a aplicação e a conformidade com as referidas novas disposições com vista a avaliar a sua eficácia. O regulamento solicitará uma avaliação e revisão pela Comissão e a apresentação de um relatório público sobre esta matéria ao Parlamento Europeu e ao Conselho até 36 meses após a data de aplicação e, posteriormente, de quatro em quatro anos.

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

Disposições gerais (capítulo I)

A presente proposta de regulamento estabelece a) regras para a colocação no mercado de produtos com elementos digitais, a fim de garantir a cibersegurança desses produtos; b)

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

requisitos essenciais para a conceção, o desenvolvimento e a produção de produtos com elementos digitais e obrigações dos operadores económicos em relação a esses produtos no que diz respeito à cibersegurança; c) requisitos essenciais para os processos de tratamento das vulnerabilidades aplicados pelos fabricantes para assegurar a cibersegurança dos produtos com elementos digitais durante todo o ciclo de vida, bem como obrigações dos operadores económicos em relação a estes processos; d) regras relativas à fiscalização do mercado e à aplicação das regras e requisitos acima referidos.

O regulamento proposto será aplicável a todos os produtos com elementos digitais cuja utilização prevista e razoavelmente previsível inclua uma conexão de dados lógica ou física, direta ou indireta, a um dispositivo ou rede.

O regulamento proposto não será aplicável aos produtos com elementos digitais abrangidos pelo âmbito de aplicação do Regulamento (UE) 2017/745 [dispositivos médicos para uso humano e acessórios para esses dispositivos] e do Regulamento (UE) 2017/746 [dispositivos médicos para diagnóstico *in vitro* para uso humano e acessórios desses dispositivos], uma vez que ambos os regulamentos preveem requisitos relativos a dispositivos, incluindo em matéria de *software* e obrigações gerais dos fabricantes, abrangendo todo o ciclo de vida dos produtos, bem como procedimentos de avaliação da conformidade. O presente regulamento não será aplicável aos produtos com elementos digitais que tenham sido certificados em conformidade com o Regulamento (UE) 2018/1139 [nível elevado e uniforme de segurança da aviação civil], nem aos produtos aos quais se aplica o Regulamento (UE) 2019/2144 [relativo aos requisitos de homologação dos veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos].

Os produtos críticos com elementos digitais devem estar sujeitos a procedimentos de avaliação da conformidade específicos e ser divididos nas classes I e II, tal como estabelecido no anexo III, de modo a refletir o seu nível de risco de cibersegurança, representando a classe II um risco mais elevado. Um produto com elementos digitais é considerado crítico e, por conseguinte, incluído no anexo III, atendendo ao impacto das potenciais vulnerabilidades de cibersegurança incluídas no produto com elementos digitais. A funcionalidade do produto com elementos digitais relacionada com a cibersegurança e a utilização prevista em ambientes sensíveis, nomeadamente em contexto industrial, são tidas em conta na determinação do risco de cibersegurança.

A Comissão fica igualmente habilitada a adotar atos delegados a fim de completar o presente regulamento especificando as categorias de produtos altamente críticos com elementos digitais para as quais se exige que os fabricantes obtenham um certificado europeu de cibersegurança ao abrigo de um sistema europeu de certificação da cibersegurança de modo a demonstrar a conformidade com os requisitos essenciais constantes do anexo I, ou partes dos mesmos. Ao determinar essas categorias de produtos altamente críticos com elementos digitais, a Comissão deve ter em conta o nível de risco de cibersegurança associado à categoria de produtos com elementos digitais, à luz de um ou vários dos critérios considerados para a inclusão de produtos críticos com elementos digitais no anexo III, bem como tendo em vista avaliar se essa categoria de produtos é utilizada ou serve de base às entidades essenciais do tipo referido no anexo [anexo I] da Diretiva [Diretiva XXX/XXXX (SRI 2)] ou se é suscetível de ter importância futura para as atividades dessas entidades; ou se é relevante para a resiliência da cadeia de abastecimento global dos produtos com elementos digitais face a acontecimentos disruptivos.

Obrigações dos operadores económicos (capítulo II)

A proposta engloba obrigações para fabricantes, importadores e distribuidores com base nas disposições de referência previstas na Decisão n.º 768/2008/CE. Os requisitos e obrigações essenciais de cibersegurança exigem que todos os produtos com elementos digitais só sejam disponibilizados no mercado se, quando devidamente fornecidos, corretamente instalados,

mantidos e utilizados para a finalidade prevista ou em condições razoavelmente previsíveis, cumprirem os requisitos essenciais de cibersegurança estabelecidos no presente regulamento.

Os requisitos e obrigações essenciais exigirão que os fabricantes tenham em conta a cibersegurança na conceção, no desenvolvimento e na produção dos produtos com elementos digitais, exerçam a devida diligência sobre os aspetos de segurança aquando da conceção e do desenvolvimento dos seus produtos, sejam transparentes sobre os aspetos de cibersegurança que devem ser comunicados aos clientes, assegurem o apoio prestado no domínio da segurança (atualizações) de forma proporcionada e cumpram os requisitos de tratamento das vulnerabilidades.

Serão estabelecidas obrigações para os operadores económicos, desde os fabricantes até aos distribuidores e importadores, no que respeita à colocação no mercado de produtos com elementos digitais, de acordo com as suas funções e responsabilidades na cadeia de abastecimento.

Conformidade do produto com elementos digitais (capítulo III)

Presume-se que o produto com elementos digitais que está em conformidade com as normas harmonizadas ou partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, esteja conforme com os requisitos essenciais da presente proposta de regulamento. Caso não existam normas harmonizadas ou estas sejam insuficientes, ou caso se verifiquem atrasos indevidos no procedimento de normalização ou o pedido da Comissão não tenha sido aceite pelas organizações europeias de normalização, a Comissão pode, por meio de atos de execução, adotar especificações comuns.

Além disso, presume-se que os produtos com elementos digitais que tenham sido certificados ou para os quais tenha sido emitida uma declaração de conformidade ou um certificado UE no âmbito de um sistema europeu de certificação da cibersegurança nos termos do Regulamento (UE) 2019/881, e relativamente aos quais a Comissão tenha especificado, por meio de um ato de execução, que pode conferir presunção de conformidade com o presente regulamento, cumprem os requisitos essenciais do presente regulamento, ou partes destes, contanto que a declaração de conformidade da UE ou o certificado de cibersegurança, ou partes destes, abranjam esses requisitos.

Ademais, a fim de evitar encargos administrativos indevidos para os fabricantes, se for caso disso, a Comissão deve especificar se um certificado de cibersegurança emitido ao abrigo desse sistema europeu de certificação da cibersegurança elimina a obrigação de os fabricantes realizarem uma avaliação da conformidade por terceiros, tal como previsto no presente regulamento para os requisitos correspondentes.

O fabricante deve realizar uma avaliação da conformidade do produto com elementos digitais e dos processos de tratamento das vulnerabilidades que aplicou para demonstrar a conformidade com os requisitos essenciais estabelecidos no anexo I, seguindo um dos procedimentos previstos no anexo VI. Os fabricantes de produtos críticos das classes I e II devem utilizar os respetivos módulos necessários para a conformidade. Os fabricantes de produtos críticos da classe II devem recorrer a um terceiro para realizar a sua avaliação da conformidade.

Notificação dos organismos de avaliação da conformidade (capítulo IV)

O funcionamento adequado dos organismos notificados é crucial para assegurar um elevado nível de cibersegurança e para a confiança de todas as partes interessadas no sistema da nova abordagem. Por conseguinte, em conformidade com a Decisão 768/2008/CE, a proposta estabelece os requisitos aplicáveis às autoridades nacionais responsáveis pelos organismos de avaliação da conformidade (organismos notificados). É deixada aos Estados-Membros a responsabilidade final de designar e controlar os organismos notificados. Os Estados-Membros devem designar uma autoridade notificadora responsável pela instauração e pela

execução dos procedimentos necessários para a avaliação e a notificação dos organismos de avaliação da conformidade, bem como pelo controlo dos organismos notificados.

Fiscalização do mercado e aplicação da legislação (capítulo V)

Em conformidade com o Regulamento (UE) 2019/1020, as autoridades nacionais de fiscalização do mercado realizam a fiscalização do mercado no território do respetivo Estado-Membro. Os Estados-Membros podem optar por designar qualquer autoridade existente ou nova para atuar como autoridade de fiscalização do mercado, incluindo as autoridades nacionais competentes estabelecidas no artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)] ou as autoridades nacionais de certificação da cibersegurança designadas a que se refere o artigo 58.º do Regulamento (UE) 2019/881. Os operadores económicos são convidados a cooperar plenamente com as autoridades de fiscalização do mercado e outras autoridades competentes.

Poderes delegados e procedimentos de comité (capítulo VI)

A fim de assegurar que o quadro regulamentar possa ser adaptado sempre que necessário, o poder de adotar atos nos termos do artigo 290.º do TFUE é delegado na Comissão para atualizar a lista de produtos críticos das classes I e II e especificar as definições destes produtos; especificar se é necessária uma limitação ou exclusão para produtos com elementos digitais abrangidos por outras regras da União que estabeleçam requisitos suscetíveis de alcançar o mesmo nível de proteção do presente regulamento; impor a certificação de determinados produtos altamente críticos com elementos digitais com base nos critérios estabelecidos no presente regulamento; especificar o conteúdo mínimo da declaração de conformidade UE e completar os elementos a incluir na documentação técnica.

A Comissão fica igualmente habilitada a adotar atos de execução para: especificar o formato ou os elementos das obrigações de informação e da lista de materiais do *software*; especificar os sistemas europeus de certificação da cibersegurança que podem ser utilizados para demonstrar a conformidade com os requisitos essenciais ou partes dos mesmos estabelecidos no presente regulamento; adotar especificações comuns; estabelecer especificações técnicas para a aposição da marcação CE; adotar medidas corretivas ou restritivas a nível da União em circunstâncias excecionais que justifiquem uma intervenção imediata para preservar o bom funcionamento do mercado interno.

Confidencialidade e sanções (capítulo VII)

Todas as partes envolvidas na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no desempenho das suas funções e atividades.

A fim de assegurar a aplicação efetiva das obrigações estabelecidas no presente regulamento, cada autoridade de fiscalização do mercado deve ter poderes para impor ou solicitar a imposição de coimas. Pela mesma ordem de ideias, o presente regulamento estabelece níveis máximos para as coimas administrativas que devem ser previstos na legislação nacional em caso de incumprimento das obrigações estabelecidas no presente regulamento.

Disposições transitórias e finais (capítulo VIII)

A fim de permitir que os fabricantes, os organismos notificados e os Estados-Membros disponham de tempo para se adaptarem aos novos requisitos, o regulamento proposto será aplicável [24 meses] após a sua entrada em vigor, com exceção da obrigação de comunicação de informações imposta aos fabricantes, que será aplicável a partir de [12 meses] após a data de entrada em vigor.

2022/0272 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

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

Tendo em conta o parecer do Comité das Regiões[2],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) É necessário melhorar o funcionamento do mercado interno estabelecendo um quadro jurídico uniforme para os requisitos essenciais de cibersegurança aplicáveis à colocação de produtos com elementos digitais no mercado da União. Importa resolver dois problemas importantes que aumentam os custos para os utilizadores e para a sociedade: o baixo nível de cibersegurança dos produtos com elementos digitais, que se traduz em vulnerabilidades generalizadas e na oferta insuficiente e incoerente de atualizações de segurança para as resolver, e o entendimento e acesso deficientes dos utilizadores à informação, que os impede de escolher produtos com propriedades de cibersegurança adequadas ou de os utilizar de forma segura.

(2) O presente regulamento visa estabelecer as condições-limite para o desenvolvimento de produtos com elementos digitais seguros, garantindo que sejam colocados no mercado produtos de *hardware* e *software* com menos vulnerabilidades e que os fabricantes encarem a segurança com seriedade ao longo de todo o ciclo de vida de um produto. Pretende ainda criar condições que permitam aos utilizadores ter em conta a cibersegurança aquando da seleção e da utilização de produtos com elementos digitais.

(3) A legislação pertinente da União atualmente em vigor contempla vários conjuntos de regras horizontais que abordam determinados aspetos relacionados com a cibersegurança a partir de diferentes ângulos, incluindo medidas para melhorar a segurança da cadeia de abastecimento digital. No entanto, a legislação da União em vigor em matéria de cibersegurança, nomeadamente a [Diretiva XXX/XXXX (SRI 2)]

[1] JO C de , p. .
[2] JO C de , p. .

e o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[3], não abrange diretamente os requisitos obrigatórios de segurança dos produtos com elementos digitais.

(4) Embora a legislação da União em vigor se aplique a determinados produtos com elementos digitais, não existe um quadro regulamentar horizontal da União que estabeleça requisitos abrangentes de cibersegurança para todos os produtos com elementos digitais. Os diversos atos e iniciativas adotados até à data a nível da União e a nível nacional apenas abordam parcialmente os problemas e riscos identificados relacionados com a cibersegurança, criando um mosaico legislativo no mercado interno, aumentando a insegurança jurídica tanto para os fabricantes como para os utilizadores desses produtos e impondo desnecessariamente mais encargos às empresas no cumprimento de uma série de requisitos para tipos semelhantes de produtos. A cibersegurança destes produtos tem uma dimensão transfronteiriça particularmente forte, uma vez que os produtos fabricados num país são muitas vezes utilizados por organizações e consumidores em todo o mercado interno, o que torna necessário regulamentar este domínio a nível da União. O panorama regulamentar da União deve ser harmonizado através da introdução de requisitos de cibersegurança para os produtos com elementos digitais. Além disso, há que garantir segurança aos operadores e utilizadores em toda a União, assim como uma melhor harmonização do mercado único, criando condições mais viáveis para os operadores que pretendam entrar no mercado da União.

(5) A nível da União, vários documentos programáticos e políticos, como a Estratégia de Cibersegurança da UE para a Década Digital[4], as Conclusões do Conselho de 2 de dezembro de 2020 e de 23 de maio de 2022 ou a Resolução do Parlamento Europeu de 10 de junho de 2021[5], apelaram à criação de requisitos específicos da União em matéria de cibersegurança para produtos digitais ou conectados, sendo que vários países em todo o mundo introduziram medidas para resolver esta questão por sua própria iniciativa. No relatório final da Conferência sobre o Futuro da Europa[6], os cidadãos apelaram ao reforço do papel da UE na luta contra as ameaças à cibersegurança.

(6) A fim de aumentar o nível global de cibersegurança de todos os produtos com elementos digitais colocados no mercado interno, é necessário introduzir requisitos essenciais de cibersegurança para estes produtos, que sejam orientados para objetivos, tecnologicamente neutros e horizontalmente aplicáveis.

(7) Em determinadas condições, todos os produtos com elementos digitais integrados ou conectados a um sistema de informação eletrónico de maior dimensão podem servir de vetor de ataque a agentes mal-intencionados. Consequentemente, mesmo o *hardware* e o *software* considerados menos críticos podem resultar no comprometimento inicial de

---

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

[4] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=JOIN:2020:18:FIN.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_PT.html.

[6] *Conference on the Future of Europe – Report on the Final Outcome*, maio de 2022, proposta 28, ponto 2. A conferência teve lugar entre abril de 2021 e maio de 2022. Tratou-se de um exercício único, liderado pelos cidadãos, de democracia deliberativa a nível pan-europeu, envolvendo milhares de cidadãos europeus, bem como intervenientes políticos, parceiros sociais, representantes da sociedade civil e principais partes interessadas.

um dispositivo ou rede, permitindo que agentes mal-intencionados obtenham acesso privilegiado a um sistema ou circulem lateralmente entre sistemas. Os fabricantes devem, por conseguinte, assegurar que todos os produtos conectáveis com elementos digitais sejam concebidos e desenvolvidos em conformidade com os requisitos essenciais estabelecidos no presente regulamento. Tal inclui os produtos que podem ser conectados fisicamente através de interfaces de *hardware* e os produtos que estão conectados logicamente, como interconectores, tubos, ficheiros, interfaces de programação de aplicações ou quaisquer outros tipos de interface de *software*. Uma vez que as ameaças à cibersegurança podem propagar-se através de vários produtos com elementos digitais antes de alcançar um determinado objetivo, encadeando, por exemplo, múltiplas ações de exploração de vulnerabilidades, os fabricantes devem também garantir a cibersegurança desses produtos que só estão indiretamente conectados a outros dispositivos ou redes.

(8) O estabelecimento de requisitos de cibersegurança para a colocação de produtos com elementos digitais no mercado reforça a cibersegurança destes produtos tanto para os consumidores como para as empresas. Estes incluem igualmente requisitos para a colocação no mercado de produtos de consumo com elementos digitais destinados a consumidores vulneráveis, tais como brinquedos e dispositivos de vigilância de bebés.

(9) O presente regulamento assegura um elevado nível de cibersegurança dos produtos com elementos digitais. Não regulamenta serviços, como o *software* como serviço (*software-as-a-service* – SaaS), com exceção das soluções de tratamento remoto de dados relativas a produtos com elementos digitais, entendidas como qualquer tratamento de dados à distância para o qual o *software* tenha sido concebido e desenvolvido pelo fabricante dos produtos em causa ou sob a sua responsabilidade e cuja inexistência impediria os produtos com elementos digitais de desempenhar uma das suas funções. A [Diretiva XXX/XXXX (SRI 2)] estabelece requisitos de cibersegurança e de notificação de incidentes para entidades essenciais e importantes, como as infraestruturas críticas, com vista a aumentar a resiliência dos serviços que prestam. A [Diretiva XXX/XXXX (SRI 2)] é aplicável aos serviços de computação em nuvem e aos modelos de serviços de computação em nuvem, como o SaaS. Todas as entidades que prestam serviços de computação em nuvem na União que atinjam ou excedam o limiar para as médias empresas são abrangidas pelo âmbito de aplicação da referida diretiva.

(10) A fim de não prejudicar a inovação ou a investigação, o *software* livre e de código fonte aberto desenvolvido ou fornecido à margem do exercício de uma atividade comercial não deve ser abrangido pelo presente regulamento. É o que acontece, em especial, com o *software*, incluindo os respetivos código-fonte e versões modificadas, que é partilhado abertamente e é de acesso, utilização, modificação e redistribuição livres. No contexto do *software*, uma atividade comercial pode caracterizar-se não só pela cobrança de um preço por um produto, mas também pela cobrança de um preço pelos serviços de apoio técnico, pela disponibilização de uma plataforma de *software* através da qual o fabricante lucre com outros serviços, ou pela utilização de dados pessoais por razões que não sejam exclusivamente destinadas a melhorar a segurança, a compatibilidade ou a interoperabilidade do *software*.

(11) Uma Internet segura é indispensável para o funcionamento das infraestruturas críticas e para a sociedade no seu conjunto. A [Diretiva XXX/XXXX (SRI 2)] visa garantir um elevado nível de cibersegurança aos serviços prestados por entidades essenciais e importantes, incluindo os fornecedores de infraestruturas digitais que apoiam as funções essenciais da Internet aberta e asseguram o acesso à Internet e os serviços de

Internet. Por conseguinte, é importante que os produtos com elementos digitais necessários para que os fornecedores de infraestruturas digitais garantam o funcionamento da Internet sejam desenvolvidos de forma segura e cumpram normas de segurança da Internet bem definidas. O presente regulamento, que se aplica a todos os produtos conectáveis de *hardware* e *software*, visa igualmente facilitar a conformidade dos fornecedores de infraestruturas digitais com os requisitos da cadeia de abastecimento previstos na [Diretiva XXX/XXXX (SRI 2)], garantindo que os produtos com elementos digitais que utilizam para a prestação dos seus serviços sejam desenvolvidos de forma segura, bem como o seu acesso a atualizações de segurança atempadas para esses produtos.

(12) O Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho[7] estabelece regras relativas aos dispositivos médicos e o Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho[8] estabelece regras relativas aos dispositivos médicos para diagnóstico *in vitro*. Ambos os regulamentos abordam os riscos de cibersegurança e seguem abordagens específicas que também são contempladas no presente regulamento. Mais especificamente, os Regulamentos (UE) 2017/745 e (UE) 2017/746 estabelecem requisitos essenciais para os dispositivos médicos que funcionam através de um sistema eletrónico ou que constituem, por si mesmos, *software*. Os referidos regulamentos abrangem igualmente certos tipos de *software* não incorporado, bem como a abordagem de todo o ciclo de vida. Estes requisitos obrigam os fabricantes a desenvolver e construir os seus produtos aplicando princípios de gestão dos riscos e estabelecendo requisitos de segurança informática, bem como os correspondentes procedimentos de avaliação da conformidade. Além disso, desde dezembro de 2019, existem diretrizes específicas em matéria de cibersegurança dos dispositivos médicos, que fornecem aos fabricantes de dispositivos médicos, incluindo dispositivos para diagnóstico *in vitro*, orientações sobre a forma de cumprir todos os requisitos essenciais pertinentes do anexo I desses regulamentos no que diz respeito à cibersegurança[9]. Os produtos com elementos digitais a que se aplique qualquer um desses regulamentos não devem, por conseguinte, ser abrangidos pelo presente regulamento.

(13) O Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho[10] estabelece requisitos de homologação de veículos e dos seus sistemas e componentes,

---

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

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

9 MDCG 2019-16, aprovado pelo Grupo de Coordenação dos Dispositivos Médicos (MDCG) criado pelo artigo 103.º do Regulamento (UE) 2017/745.

10 Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1).

introduzindo determinados requisitos de cibersegurança, nomeadamente no que respeita ao funcionamento de um sistema de gestão da cibersegurança certificado e às atualizações de *software*, abrangendo políticas e processos das organizações em matéria de riscos cibernéticos relacionados com todo o ciclo de vida dos veículos, equipamentos e serviços, em conformidade com os regulamentos das Nações Unidas aplicáveis em matéria de especificações técnicas e cibersegurança[11], e prevendo procedimentos específicos de avaliação da conformidade. No domínio da aviação, o Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho[12] tem como objetivo principal estabelecer e manter um nível elevado e uniforme de segurança da aviação civil na União. Cria um quadro para os requisitos essenciais de aeronavegabilidade dos produtos, peças e equipamentos aeronáuticos, incluindo o *software*, que tem em conta as obrigações de proteção contra ameaças à segurança da informação. Os produtos com elementos digitais aos quais se aplica o Regulamento (UE) 2019/2144 e os produtos certificados em conformidade com o Regulamento (UE) 2018/1139 não estão, por conseguinte, sujeitos aos requisitos essenciais e aos procedimentos de avaliação da conformidade estabelecidos no presente regulamento. O processo de certificação previsto no Regulamento (UE) 2018/1139 assegura o nível de garantia visado no presente regulamento.

(14) O presente regulamento estabelece regras horizontais em matéria de cibersegurança que não se aplicam especificamente a setores ou a determinados produtos com elementos digitais. No entanto, poderão ser introduzidas regras da União setoriais ou específicas para determinados produtos, que estabeleçam requisitos que abranjam a totalidade ou parte dos riscos contemplados nos requisitos essenciais estabelecidos no presente regulamento. Em tais casos, a aplicação do presente regulamento a produtos com elementos digitais abrangidos por outras regras da União, que estabeleçam requisitos que tenham em conta a totalidade ou parte dos riscos contemplados pelos requisitos essenciais estabelecidos no anexo I do presente regulamento, pode ser limitada ou excluída se essa limitação ou exclusão for coerente com o quadro regulamentar global aplicável a esses produtos e se as regras setoriais permitirem alcançar o mesmo nível de proteção que o previsto no presente regulamento. A Comissão fica habilitada a adotar atos delegados para alterar o presente regulamento, identificando os referidos produtos e regras. O presente regulamento contém disposições específicas que clarificam a sua relação com a legislação da União em vigor que implique a aplicação dessas limitações ou exclusões.

(15) O Regulamento Delegado (UE) 2022/30 especifica que os requisitos essenciais estabelecidos no artigo 3.º, n.º 3, alínea d) (danos na rede e utilização inadequada dos recursos da rede), alínea e) (dados pessoais e privacidade) e alínea f) (fraude), da Diretiva 2014/53/UE se aplicam a determinados equipamentos de rádio. A [Decisão de execução XXX/2022 da Comissão relativa a um pedido de normalização às organizações europeias de normalização] estabelece requisitos para o desenvolvimento de normas específicas que definam melhor a forma como estes três requisitos

---

11 Regulamento n.º 155 da ONU — Prescrições uniformes relativas à homologação de veículos no que diz respeito à cibersegurança e ao sistema de gestão da cibersegurança [2021/387].

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

essenciais devem ser tratados. Os requisitos essenciais estabelecidos no presente regulamento incluem todos os elementos dos requisitos essenciais referidos no artigo 3.º, n.º 3, alíneas d), e) e f), da Diretiva 2014/53/UE. Além disso, os requisitos essenciais estabelecidos no presente regulamento harmonizam-se com os objetivos dos requisitos para a elaboração de normas específicas incluídos nesse pedido de normalização. Por conseguinte, se a Comissão revogar ou alterar o Regulamento Delegado (UE) 2022/30 e, consequentemente, este deixar de se aplicar a determinados produtos abrangidos pelo presente regulamento, a Comissão e as organizações europeias de normalização devem ter em conta o trabalho de normalização realizado no contexto da Decisão de Execução C(2022)5637 da Comissão relativa a um pedido de normalização para o Regulamento Delegado 2022/30 da DER na elaboração e no desenvolvimento de normas harmonizadas para facilitar a aplicação do presente regulamento.

(16) A Diretiva 85/374/CEE[13] complementa o presente regulamento. Essa diretiva estabelece regras em matéria de responsabilidade decorrente de produtos defeituosos de modo que as pessoas lesadas possam exigir uma indemnização quando um dano tiver sido causado por produtos defeituosos. Estabelece o princípio de que o fabricante de um produto é responsável pelos danos causados pela falta de segurança do seu produto, independentemente da existência de culpa («responsabilidade objetiva»). Sempre que uma tal ausência de segurança consistir numa falta de atualizações de segurança após a colocação do produto no mercado e esta cause danos, a responsabilidade do fabricante poderá ser acionada. As obrigações dos fabricantes que digam respeito ao fornecimento dessas atualizações de segurança devem ser estabelecidas no presente regulamento.

(17) O presente regulamento não deve prejudicar o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[14], incluindo as disposições relativas ao estabelecimento de procedimentos de certificação em matéria de proteção de dados e de selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o referido regulamento. Tais operações poderão ser incorporadas num produto com elementos digitais. A proteção de dados desde a conceção e por defeito, bem como a cibersegurança em geral, são elementos fundamentais do Regulamento (UE) 2016/679. Ao proteger os consumidores e as organizações contra os riscos de cibersegurança, os requisitos essenciais de cibersegurança estabelecidos no presente regulamento devem também contribuir para reforçar a proteção dos dados pessoais e da privacidade das pessoas. Importa ponderar o desenvolvimento de sinergias, tanto em matéria de normalização como de certificação dos aspetos de cibersegurança, através da cooperação entre a Comissão, as organizações europeias de normalização, a Agência da União Europeia para a Cibersegurança (ENISA), o Comité Europeu para a Proteção de Dados (CEPD), criado pelo Regulamento (UE) 2016/679, e as autoridades nacionais de controlo da proteção de dados. Devem também ser criadas sinergias entre o presente regulamento

---

13 Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos (JO L 210 de 7.8.1985).

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

e a legislação da União em matéria de proteção de dados no domínio da fiscalização do mercado e da execução. Para o efeito, as autoridades nacionais de fiscalização do mercado designadas ao abrigo do presente regulamento devem cooperar com as autoridades responsáveis pela supervisão da legislação da União em matéria de proteção de dados. Estas últimas devem igualmente ter acesso às informações pertinentes para o desempenho das suas funções.

(18) Na medida em que os seus produtos sejam abrangidos pelo âmbito de aplicação do presente regulamento, os emitentes de carteiras europeias de identidade digital a que se refere o artigo [artigo 6.º-A, n.º 2, do Regulamento (UE) n.º 910/2014, com a redação que lhe foi dada pela proposta de regulamento que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação de um quadro europeu para a identidade digital], devem cumprir os requisitos essenciais horizontais estabelecidos no presente regulamento e os requisitos de segurança específicos estabelecidos no artigo [artigo 6.º-A do Regulamento (UE) n.º 910/2014, com a redação que lhe foi dada pela proposta de regulamento que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação de um quadro europeu para a identidade digital]. A fim de facilitar o cumprimento, os emitentes de carteiras digitais devem poder demonstrar a conformidade das carteiras europeias de identidade digital com os requisitos estabelecidos, respetivamente, em ambos os atos, certificando os seus produtos no âmbito de um sistema europeu de certificação da cibersegurança criado nos termos do Regulamento (UE) 2019/881 e relativamente ao qual a Comissão tenha especificado, através de um ato de execução, uma presunção de conformidade com o presente regulamento, contanto que o certificado, ou partes do mesmo, abranja esses requisitos.

(19) Determinadas funções previstas no presente regulamento devem ser desempenhadas pela ENISA, nos termos do artigo 3.º, n.º 2, do Regulamento (UE) 2019/881. Em especial, a ENISA deve receber notificações dos fabricantes a respeito de vulnerabilidades ativamente exploradas existentes nos produtos com elementos digitais, bem como de incidentes com impacto na segurança desses produtos. A ENISA deve igualmente transmitir essas notificações às equipas de resposta a incidentes de segurança informática (CSIRT) pertinentes ou, respetivamente, aos pontos de contacto únicos pertinentes dos Estados-Membros designados em conformidade com o artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)], e informar as autoridades de fiscalização do mercado competentes sobre a vulnerabilidade notificada. Com base nas informações que recolhe, a ENISA deve elaborar, de dois em dois anos, um relatório técnico sobre as tendências emergentes em matéria de riscos de cibersegurança de produtos com elementos digitais e apresentá-lo ao grupo de cooperação referido na Diretiva [Diretiva XXX/XXXX (SRI 2)]. Além disso, tendo em conta os seus conhecimentos especializados e o seu mandato, a ENISA deve poder apoiar o processo de aplicação do presente regulamento. Em especial, deve poder propor atividades conjuntas a realizar pelas autoridades de fiscalização do mercado, com base em indícios ou informações sobre a potencial não conformidade de produtos com elementos digitais em vários Estados-Membros com o presente regulamento, ou identificar categorias de produtos para as quais devam ser organizadas ações de controlo coordenadas simultâneas. Em circunstâncias excecionais, a pedido da Comissão, a ENISA deve poder realizar avaliações de produtos específicos com elementos digitais que apresentem um risco de cibersegurança significativo, caso seja necessária uma intervenção imediata para preservar o bom funcionamento do mercado interno.

(20) Para que possam circular livremente dentro do mercado interno, os produtos com elementos digitais devem apresentar a marcação CE para indicar o cumprimento do presente regulamento. Os Estados-Membros não podem criar obstáculos injustificados à colocação no mercado de produtos com elementos digitais que cumpram os requisitos previstos no presente regulamento e apresentem a marcação CE.

(21) A fim de assegurar que os fabricantes possam lançar *software* para fins de ensaio antes de submeterem os seus produtos a uma avaliação da conformidade, os Estados-Membros não devem impedir a disponibilização de *software* inacabado, como versões alfa, versões beta ou candidatos a lançamento, contanto que a versão só seja disponibilizada durante o tempo necessário para testá-la e recolher opiniões. Os fabricantes devem assegurar que o *software* disponibilizado nestas condições só seja lançado na sequência de uma avaliação dos riscos e que cumpra, na medida do possível, os requisitos de segurança relativos às propriedades dos produtos com elementos digitais impostos pelo presente regulamento. Os fabricantes devem também aplicar, na medida do possível, os requisitos de tratamento das vulnerabilidades. Os fabricantes não devem obrigar os utilizadores à atualização para versões lançadas apenas para fins de ensaio.

(22) A fim de assegurar que, uma vez colocados no mercado, os produtos com elementos digitais não acarretem riscos de cibersegurança para as pessoas e as organizações, devem ser estabelecidos requisitos essenciais para esses produtos. Quando os produtos forem subsequentemente modificados, através de meios físicos ou digitais, de uma forma que não esteja prevista pelo fabricante e que possa implicar que deixem de cumprir os requisitos essenciais pertinentes, a modificação deve ser considerada substancial. Por exemplo, as atualizações ou reparações de *software* podem ser equiparadas a operações de manutenção, desde que não modifiquem um produto já colocado no mercado de tal maneira que possam afetar a conformidade com os requisitos aplicáveis ou alterar a utilização prevista para a qual o produto foi avaliado. Tal como acontece com as reparações ou modificações físicas, um produto com elementos digitais deve ser considerado substancialmente modificado por uma alteração do *software* quando a atualização do *software* alterar as funções, o tipo ou o desempenho inicialmente previstos do produto e essas alterações não estiverem previstas na avaliação dos risco inicial, quando a natureza do perigo se tiver alterado ou quando o nível de risco tiver aumentado devido à atualização do *software*.

(23) Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, sempre que ocorra uma alteração substancial que possa afetar a conformidade de um produto com o presente regulamento ou quando a finalidade prevista desse produto se altere, é conveniente verificar a conformidade do produto com elementos digitais e, se for caso disso, submetê-lo uma nova avaliação da conformidade. Se aplicável, caso o fabricante proceda a uma avaliação da conformidade que envolva terceiros, deve notificar-lhes as alterações que possam conduzir a modificações substanciais.

(24) O recondicionamento, a manutenção e a reparação de um produto com elementos digitais, tal como definidos no Regulamento [Regulamento Conceção Ecológica], não conduzem necessariamente a uma modificação substancial do produto se, por exemplo, a utilização e as funcionalidades previstas não forem alteradas e o nível de risco não for afetado. No entanto, a atualização de um produto pelo fabricante pode conduzir a alterações na conceção e no desenvolvimento do produto e, por conseguinte, afetar a sua utilização prevista e a sua conformidade com os requisitos estabelecidos no presente regulamento.

(25) Os produtos com elementos digitais devem ser considerados críticos se o impacto negativo da exploração de potenciais vulnerabilidades de cibersegurança no produto for potencialmente grave devido, entre outras razões, à funcionalidade relacionada com a cibersegurança ou à utilização prevista. Em especial, as vulnerabilidades de produtos com elementos digitais com uma funcionalidade relacionada com a cibersegurança, como elementos seguros, por exemplo, podem conduzir a uma multiplicação dos problemas de segurança em toda a cadeia de abastecimento. A gravidade do impacto de um incidente de cibersegurança pode também aumentar se for tida em conta a utilização prevista do produto, por exemplo, num contexto industrial, no contexto de uma entidade essencial do tipo referido no anexo [anexo I] da Diretiva [Diretiva XXX/XXXX (SRI 2)], ou para o desempenho de funções críticas ou sensíveis, como o tratamento de dados pessoais.

(26) Os produtos críticos com elementos digitais devem ser objeto de procedimentos de avaliação da conformidade mais rigorosos, sem deixar de manter uma abordagem proporcionada. Para o efeito, os produtos críticos com elementos digitais devem ser divididos em duas classes que reflitam o nível de risco de cibersegurança associado a estas categorias de produtos. Um potencial ciberincidente que envolva produtos da classe II pode ter impactos negativos mais graves do que um incidente que envolva produtos da classe I devido, por exemplo, à natureza da sua função relacionada com a cibersegurança ou à sua utilização prevista em ambientes sensíveis, devendo, por conseguinte, ser objeto de um procedimento de avaliação da conformidade mais rigoroso.

(27) As categorias de produtos críticos com elementos digitais referidas no anexo III do presente regulamento devem ser entendidas como os produtos cuja funcionalidade principal é do tipo indicado no anexo III do presente regulamento. Por exemplo, o anexo III do presente regulamento enumera os produtos que são definidos de acordo com a sua funcionalidade principal como microprocessadores de uso geral pertencentes à classe II. Consequentemente, os microprocessadores de uso geral estão sujeitos a uma avaliação obrigatória da conformidade por terceiros. Não é este o caso de outros produtos não explicitamente referidos no anexo III do presente regulamento que possam integrar um microprocessador de uso geral. A Comissão deve adotar atos delegados [no prazo de 12 meses a contar da data de entrada em vigor do presente regulamento] para especificar as definições das categorias de produtos abrangidas pelas classes I e II estabelecidas no anexo III.

(28) O presente regulamento aborda os riscos de cibersegurança de forma direcionada. No entanto, os produtos com elementos digitais podem apresentar outros riscos para a segurança não relacionados com a cibersegurança. Esses riscos devem continuar a ser regulamentados por outra legislação pertinente da União em matéria de produtos. Se não for aplicável outra legislação de harmonização da União, devem estar sujeitos ao Regulamento [Regulamento Segurança Geral dos Produtos]. Por conseguinte, tendo em conta a natureza específica do presente regulamento, em derrogação do artigo 2.º, n.º 1, terceiro parágrafo, alínea b), do Regulamento [Regulamento Segurança Geral dos Produtos], o capítulo III, secção 1, os capítulos V e VII e os capítulos IX a XI do Regulamento [Regulamento Segurança Geral dos Produtos] devem aplicar-se aos produtos com elementos digitais no que diz respeito aos riscos de segurança não abrangidos pelo presente regulamento, se esses produtos não estiverem sujeitos a requisitos específicos impostos por outra legislação de harmonização da União, na aceção do [artigo 3.º, n.º 25, do Regulamento Segurança Geral dos Produtos].

(29) Os produtos com elementos digitais classificados como sistemas de IA de risco elevado nos termos do artigo 6.º do Regulamento[15] [Regulamento Inteligência Artificial] abrangidos pelo âmbito de aplicação do presente regulamento devem cumprir os requisitos essenciais estabelecidos no presente regulamento. Quando esses sistemas de IA de risco elevado cumprem os requisitos essenciais do presente regulamento, devem ser considerados conformes com os requisitos de cibersegurança estabelecidos no artigo [artigo 15.º] do Regulamento [Regulamento Inteligência Artificial], contanto que esses requisitos estejam abrangidos pela declaração de conformidade UE ou partes da mesma emitida ao abrigo do presente regulamento. No que diz respeito aos procedimentos de avaliação da conformidade relacionados com os requisitos essenciais de cibersegurança de um produto com elementos digitais abrangido pelo presente regulamento e classificado como um sistema de IA de risco elevado, as disposições pertinentes do artigo 43.º do Regulamento [Regulamento Inteligência Artificial] devem, em regra, aplicar-se em vez das disposições correspondentes do presente regulamento. No entanto, esta regra não deve resultar na redução do nível de garantia necessário para os produtos críticos com elementos digitais abrangidos pelo presente regulamento. Por conseguinte, em derrogação desta regra, os sistemas de IA de risco elevado abrangidos pelo âmbito de aplicação do Regulamento [Regulamento Inteligência Artificial], também qualificados como produtos críticos com elementos digitais nos termos do presente regulamento e aos quais se aplica o procedimento de avaliação da conformidade baseado no controlo interno referido no anexo VI do Regulamento [Regulamento Inteligência Artificial] devem ser sujeitos às disposições do presente regulamento em matéria de avaliação da conformidade, no que diz respeito aos requisitos essenciais do presente regulamento. Neste caso, em relação aos demais aspetos abrangidos pelo Regulamento [Regulamento Inteligência Artificial], devem aplicar-se as respetivas disposições em matéria de avaliação da conformidade com base no controlo interno estabelecidas no anexo VI do Regulamento [Regulamento Inteligência Artificial].

(30) As máquinas e seus componentes e acessórios abrangidos pelo âmbito de aplicação do Regulamento [proposta de Regulamento Máquinas] que sejam produtos com elementos digitais na aceção do presente regulamento e para os quais tenha sido emitida uma declaração de conformidade com base no presente regulamento devem ser considerados conformes com os requisitos essenciais de saúde e segurança estabelecidos no [anexo III, secções 1.1.9 e 1.2.1] do Regulamento [proposta de Regulamento Máquinas], no que diz respeito à proteção contra a corrupção e à segurança e fiabilidade dos sistemas de comando, na medida em que a conformidade com esses requisitos seja demonstrada pela declaração de conformidade UE emitida ao abrigo do presente regulamento.

(31) O Regulamento [proposta de Regulamento Espaço Europeu de Dados de Saúde] complementa os requisitos essenciais estabelecidos no presente regulamento. Os sistemas de registos de saúde eletrónicos («sistemas de RSE») abrangidos pelo âmbito de aplicação do Regulamento [proposta de Regulamento Espaço Europeu de Dados de Saúde] que sejam produtos com elementos digitais na aceção do presente regulamento devem, por conseguinte, cumprir igualmente os requisitos essenciais estabelecidos no presente regulamento. Os respetivos fabricantes devem demonstrar a conformidade, tal como exigido pelo Regulamento [proposta de Regulamento Espaço Europeu de Dados de Saúde]. A fim de facilitar a conformidade, os fabricantes podem elaborar uma

[15] Regulamento [Regulamento Inteligência Artificial].

documentação técnica única que contenha os elementos exigidos por ambos os atos jurídicos. Uma vez que o presente regulamento não abrange o SaaS enquanto tal, os sistemas de RSE disponibilizados através do modelo de licenciamento e distribuição do SaaS não são abrangidos pelo seu âmbito de aplicação. De igual modo, os sistemas de RSE desenvolvidos e utilizados internamente não são abrangidos pelo âmbito de aplicação do presente regulamento, uma vez que não são colocados no mercado.

(32) A fim de garantir a segurança dos produtos com elementos digitais tanto no momento da sua colocação no mercado como ao longo do seu ciclo de vida, é necessário estabelecer requisitos essenciais para o tratamento de vulnerabilidades, bem como requisitos essenciais de cibersegurança relativos às propriedades dos produtos com elementos digitais. Embora devam cumprir todos os requisitos essenciais relativos ao tratamento de vulnerabilidades e assegurar que todos os seus produtos sejam entregues sem quaisquer vulnerabilidades conhecidas que possam ser exploradas, os fabricantes devem determinar que outros requisitos essenciais relativos às propriedades do produto são relevantes para o tipo de produto em causa. Para o efeito, os fabricantes devem realizar uma avaliação dos riscos de cibersegurança associados a um produto com elementos digitais, a fim de identificar os riscos e os requisitos essenciais pertinentes e de aplicar de forma correta normas harmonizadas ou especificações comuns adequadas.

(33) Para melhorar a segurança dos produtos com elementos digitais colocados no mercado interno, é necessário estabelecer requisitos essenciais. Estes requisitos essenciais não devem prejudicar as avaliações coordenadas dos riscos das cadeias de abastecimento críticas a nível da UE estabelecidas pelo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)][16], que têm em conta fatores de risco técnicos e, se for caso disso, não técnicos, designadamente o exercício de influência indevida de um país terceiro sobre os fornecedores. Além disso, não devem prejudicar as prerrogativas dos Estados-Membros de estabelecer requisitos adicionais que tenham em conta fatores não técnicos com a finalidade de assegurar um elevado nível de resiliência, incluindo os definidos na Recomendação (UE) 2019/534, na avaliação coordenada dos riscos de segurança das redes 5G a nível da União e no conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G acordado pelo grupo de cooperação SRI a que se refere a [Diretiva XXX/XXXX (SRI 2)].

(34) A fim de assegurar que as CSIRT nacionais e o ponto de contacto único designado em conformidade com o artigo [artigo X] da Diretiva [Diretiva XX/XXXX (SRI 2)] recebem as informações necessárias ao desempenho das suas funções e ao reforço do nível global de cibersegurança das entidades essenciais e importantes, bem como de assegurar o funcionamento eficaz das autoridades de fiscalização do mercado, os fabricantes de produtos com elementos digitais devem notificar à ENISA vulnerabilidades que estejam a ser ativamente exploradas. Uma vez que a maioria dos produtos com elementos digitais é comercializada em todo o mercado interno, qualquer vulnerabilidade explorada num produto com elementos digitais deve ser considerada uma ameaça ao funcionamento do mercado interno. Os fabricantes devem igualmente ponderar a divulgação de vulnerabilidades corrigidas na base de dados europeia de vulnerabilidades criada ao abrigo da Diretiva [Diretiva XX/XXXX (SRI

[16] Diretiva XXX do Parlamento Europeu e do Conselho, de [data] [relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 (JO L xx de data, p. x)].

2)] e gerida pela ENISA ou em qualquer outra base de dados de vulnerabilidades acessível ao público.

(35) Os fabricantes devem também comunicar à ENISA qualquer incidente com impacto na segurança do produto com elementos digitais. Não obstante as obrigações de notificação de incidentes previstas na Diretiva [Diretiva XXX/XXXX (SRI 2)] para as entidades essenciais e importantes, é crucial que a ENISA, os pontos de contacto únicos designados pelos Estados-Membros nos termos do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)] e as autoridades de fiscalização do mercado recebam informações dos fabricantes de produtos com elementos digitais que lhes permitam avaliar a segurança desses produtos. A fim de garantir que os utilizadores possam reagir rapidamente a incidentes com impacto na segurança dos seus produtos com elementos digitais, os fabricantes devem também informar os seus utilizadores sobre qualquer incidente desse tipo e, se aplicável, sobre eventuais medidas corretivas que estes possam aplicar para atenuar o impacto do incidente, nomeadamente através da publicação de informações pertinentes nos seus sítios Web ou do contacto direto com os mesmos, caso o fabricante possa fazê-lo e sempre que os riscos o justifiquem.

(36) Os fabricantes de produtos com elementos digitais devem instituir políticas de divulgação coordenada de vulnerabilidades, a fim de facilitar a comunicação de vulnerabilidades por parte de pessoas singulares ou de entidades. Uma política de divulgação coordenada das vulnerabilidades deve especificar um processo estruturado através do qual as vulnerabilidades são comunicadas a um fabricante de uma forma que lhe permita diagnosticá-las e corrigi-las antes de serem divulgadas a terceiros ou ao público informações pormenorizadas sobre as mesmas. Dado que as informações sobre vulnerabilidades passíveis de serem exploradas em produtos com elementos digitais amplamente utilizados podem ser vendidas a preços elevados no mercado negro, os fabricantes desses produtos devem poder utilizar programas, no âmbito das suas políticas de divulgação coordenada de vulnerabilidades, para incentivar a comunicação de vulnerabilidades, assegurando que as pessoas ou entidades sejam objeto de reconhecimento e compensação pelos seus esforços (os chamados «programas de recompensas por deteção de erros de programação»).

(37) A fim de facilitar a análise de vulnerabilidades, os fabricantes devem identificar e documentar os componentes contidos nos produtos com elementos digitais, nomeadamente através da elaboração de uma lista de materiais do *software*. Uma lista de materiais do *software* pode fornecer aos fabricantes, compradores e operadores de *software* informações que melhoram a sua compreensão da cadeia de abastecimento, o que tem múltiplos benefícios, nomeadamente porque ajuda os fabricantes e os utilizadores a detetar vulnerabilidades e riscos conhecidos surgidos recentemente. É particularmente importante que os fabricantes assegurem que os seus produtos não contenham componentes vulneráveis desenvolvidos por terceiros.

(38) A fim de facilitar a avaliação da conformidade com os requisitos estabelecidos no presente regulamento, deve existir uma presunção de conformidade relativamente aos produtos com elementos digitais que estejam em conformidade com as normas harmonizadas, que traduzam os requisitos essenciais do presente regulamento em especificações técnicas pormenorizadas e que sejam adotados nos termos do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho[17]. O

[17] Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as

Regulamento (UE) n.º 1025/2012 prevê um procedimento para a apresentação de objeções às normas harmonizadas caso essas normas não satisfaçam plenamente os requisitos do presente regulamento.

(39) O Regulamento (UE) 2019/881 estabelece um quadro europeu para a certificação voluntária da cibersegurança para produtos, processos e serviços de TIC. Os sistemas europeus de certificação da cibersegurança podem incluir produtos com elementos digitais abrangidos pelo presente regulamento. O presente regulamento deve criar sinergias com o Regulamento (UE) 2019/881. A fim de facilitar a avaliação da conformidade com os requisitos estabelecidos no presente regulamento, presume-se que os produtos com elementos digitais certificados ou relativamente aos quais tenha sido emitida uma declaração de conformidade no âmbito de um sistema de cibersegurança nos termos do Regulamento (UE) 2019/881 e que tenham sido identificados pela Comissão num ato de execução estão conformes com os requisitos essenciais do presente regulamento, contanto que o certificado de cibersegurança ou a declaração de conformidade, ou partes dos mesmos, abranjam esses requisitos. Deve ser avaliada à luz do presente regulamento a necessidade de novos sistemas europeus de certificação da cibersegurança para produtos com elementos digitais. Esses futuros sistemas europeus de certificação da cibersegurança que abranjam produtos com elementos digitais devem ter em conta os requisitos essenciais estabelecidos no presente regulamento e facilitar o cumprimento do presente regulamento. A Comissão deve ficar habilitada a especificar, por meio de atos de execução, os sistemas europeus de certificação da cibersegurança que podem ser utilizados para demonstrar a conformidade com os requisitos essenciais estabelecidos no presente regulamento. Ademais, a fim de evitar encargos administrativos indevidos para os fabricantes, se for caso disso, a Comissão deve especificar se um certificado de cibersegurança emitido ao abrigo desses sistemas europeus de certificação da cibersegurança elimina a obrigação de os fabricantes realizarem uma avaliação da conformidade por terceiros, tal como previsto no presente regulamento para os requisitos correspondentes.

(40) Após a entrada em vigor do ato de execução que estabelece o [Regulamento de Execução (UE) n.º .../... da Comissão, de XXX, relativo ao sistema europeu de certificação da cibersegurança baseado em critérios comuns] (EUCC), que diz respeito aos produtos de *hardware* abrangidos pelo presente regulamento, tais como módulos de segurança físicos e microprocessadores, a Comissão pode especificar, por meio de um ato de execução, de que forma o EUCC confere uma presunção de conformidade com os requisitos essenciais a que se refere o anexo I do presente regulamento ou partes dos mesmos. Além disso, esse ato de execução pode especificar de que forma um certificado emitido no âmbito do EUCC elimina a obrigação de os fabricantes realizarem uma avaliação por terceiros, tal como exigido pelo presente regulamento para os requisitos correspondentes.

(41) Se não forem adotadas normas harmonizadas ou se as normas harmonizadas não tiverem suficientemente em conta os requisitos essenciais do presente regulamento, a Comissão deve poder adotar especificações comuns por meio de atos de execução. As razões para o desenvolvimento dessas especificações comuns, ao invés da aplicação de normas harmonizadas, podem incluir uma recusa do pedido de normalização por qualquer das organizações europeias de normalização, atrasos injustificados na

---

Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

elaboração de normas harmonizadas adequadas ou uma falta de conformidade das normas desenvolvidas com os requisitos do presente regulamento ou com um pedido da Comissão. A fim de facilitar a avaliação da conformidade com os requisitos essenciais estabelecidos no presente regulamento, deve presumir-se a conformidade dos produtos com elementos digitais que cumpram as especificações comuns adotadas pela Comissão nos termos do presente regulamento, com vista à formulação de especificações técnicas pormenorizadas para esses requisitos.

(42) Os fabricantes devem elaborar uma declaração de conformidade UE, a fim de facultar as informações exigidas pelo presente regulamento acerca da conformidade dos produtos com elementos digitais com os requisitos essenciais do presente regulamento e, sendo caso disso, de outra legislação de harmonização da União aplicável ao produto. Os fabricantes também podem ser obrigados a elaborar uma declaração de conformidade UE por outra legislação da União. Para assegurar o acesso efetivo à informação para efeitos de fiscalização do mercado, deve ser elaborada uma declaração de conformidade UE única respeitante ao cumprimento de todos os atos da União aplicáveis. A fim de reduzir os encargos administrativos que recaem sobre os operadores económicos, essa declaração de conformidade UE única deve poder ser constituída por um dossiê que contenha as várias declarações de conformidade pertinentes.

(43) A marcação CE, que indica a conformidade de um produto, é o corolário visível de todo um processo que abrange a avaliação da conformidade em sentido lato. Os princípios gerais que regem a marcação CE encontram-se definidos no Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho[18]. O presente regulamento deve definir as regras que regem a aposição da marcação CE nos produtos com elementos digitais. A marcação CE deve ser a única que garante que os produtos com elementos digitais cumprem os requisitos do presente regulamento.

(44) A fim de permitir que os operadores económicos demonstrem a conformidade com os requisitos essenciais estabelecidos no presente regulamento e que as autoridades de fiscalização do mercado assegurem que os produtos com elementos digitais disponibilizados no mercado cumpram esses requisitos, é necessário prever procedimentos de avaliação da conformidade. A Decisão 768/2008/CE do Parlamento Europeu e do Conselho[19] estabelece módulos para os procedimentos de avaliação da conformidade proporcionais ao nível de risco envolvido e ao nível de segurança exigido. A fim de assegurar a coerência intersetorial e evitar variantes *ad hoc*, os procedimentos de avaliação da conformidade adequados para verificar a conformidade dos produtos com elementos digitais com os requisitos essenciais estabelecidos no presente regulamento basearam-se nesses módulos. Os procedimentos de avaliação da conformidade devem examinar e verificar os requisitos relativos ao produto e ao processo que abrangem todo o ciclo de vida dos produtos com elementos digitais, incluindo o planeamento, a conceção, o desenvolvimento ou a produção, os ensaios e a manutenção do produto.

---

[18] Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

[19] Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE (JO L 218 de 13.8.2008, p. 82).

(45) A avaliação da conformidade dos produtos com elementos digitais deve ser realizada, regra geral, pelo fabricante sob a sua própria responsabilidade, de acordo com o procedimento baseado no módulo A da Decisão 768/2008/CE. O fabricante deve dispor de flexibilidade para escolher um procedimento de avaliação da conformidade mais rigoroso que envolva terceiros. Se o produto for classificado como produto crítico da classe I, é obrigatória uma garantia adicional para demonstrar a conformidade com os requisitos essenciais estabelecidos no presente regulamento. O fabricante deve aplicar normas harmonizadas, especificações comuns ou sistemas de certificação da cibersegurança nos termos do Regulamento (UE) 2019/881 que tenham sido identificados pela Comissão num ato de execução, caso pretenda realizar a avaliação da conformidade sob a sua própria responsabilidade (módulo A). Se não aplicar essas normas harmonizadas, especificações comuns ou sistemas de certificação da cibersegurança, o fabricante deve ser objeto de uma avaliação da conformidade por terceiros. Tendo em conta os encargos administrativos para os fabricantes e o facto de a cibersegurança desempenhar um papel importante na fase de conceção e desenvolvimento de produtos corpóreos e incorpóreos com elementos digitais, os procedimentos de avaliação da conformidade baseados, respetivamente, nos módulos B + C ou no módulo H da Decisão 768/2008/CE foram escolhidos como sendo os mais adequados para avaliar a conformidade dos produtos críticos com elementos digitais de forma proporcionada e eficaz. O fabricante cuja avaliação da conformidade seja realizada por terceiros pode escolher o procedimento que melhor corresponda ao seu processo de conceção e produção. Tendo em conta o risco de cibersegurança ainda maior associado à utilização de produtos classificados como produtos críticos da classe II, a avaliação da conformidade destes produtos deve sempre envolver terceiros.

(46) Embora a criação de produtos corpóreos com elementos digitais exija normalmente que os fabricantes desenvolvam esforços substanciais ao longo das fases de conceção, desenvolvimento e produção, a criação de produtos com elementos digitais sob a forma de *software* centra-se quase exclusivamente na conceção e no desenvolvimento, desempenhando a fase de produção um papel secundário. No entanto, em muitos casos, os produtos de *software* continuam a ter de ser compilados, construídos, embalados, disponibilizados para descarregamento ou copiados para suportes físicos antes de serem colocados no mercado. Estas atividades devem ser consideradas atividades equivalentes à produção aquando da aplicação dos módulos de avaliação da conformidade pertinentes para verificar a conformidade do produto com os requisitos essenciais do presente regulamento nas fases de conceção, desenvolvimento e produção.

(47) Para efeitos de avaliação da conformidade dos produtos com elementos digitais por terceiros, as autoridades notificadoras nacionais devem notificar os organismos de avaliação da conformidade à Comissão e aos outros Estados-Membros, contanto estes que cumpram uma série de requisitos, nomeadamente em termos de independência, competência e ausência de conflitos de interesse.

(48) Com o objetivo de garantir um nível coerente de qualidade no desempenho da avaliação da conformidade dos produtos com elementos digitais, é também necessário estabelecer requisitos a cumprir pelas autoridades notificadoras e por outros organismos envolvidos na avaliação, na notificação e no controlo dos organismos notificados. O sistema estabelecido no presente regulamento deve ser complementado pelo sistema de acreditação previsto no Regulamento (CE) n.º 765/2008. Dado que a acreditação é um meio fundamental para verificar a competência dos organismos de avaliação da conformidade, deve ser igualmente utilizada para efeitos de notificação.

(49) Uma acreditação organizada de forma transparente nos termos do Regulamento (CE) n.º 765/2008, que garanta a necessária confiança nos certificados de conformidade, deve ser considerada como o instrumento preferido das autoridades públicas nacionais em toda a União para demonstrar a competência técnica dos organismos de avaliação da conformidade. Contudo, as autoridades nacionais podem considerar que possuem os meios adequados para realizarem por si próprias essa avaliação. Nesse caso, a fim de assegurar o nível adequado de credibilidade das avaliações efetuadas por outras autoridades nacionais, aquelas devem apresentar à Comissão e aos restantes Estados-Membros as devidas provas documentais de que os organismos de avaliação da conformidade avaliados cumprem os requisitos regulamentares aplicáveis.

(50) Os organismos de avaliação da conformidade subcontratam frequentemente partes das respetivas atividades relacionadas com a avaliação da conformidade ou recorrem a filiais para esse efeito. A fim de salvaguardar o nível de proteção exigido para a colocação do produto com elementos digitais no mercado, é indispensável que esses subcontratantes e filiais que efetuam a avaliação da conformidade cumpram requisitos idênticos aos dos organismos notificados relativamente ao desempenho de tarefas de avaliação da conformidade.

(51) A notificação de um organismo de avaliação da conformidade deve ser enviada pela autoridade notificadora à Comissão e aos outros Estados-Membros através do sistema de informação NANDO (*New Approach Notified and Designated Organisations*). NANDO é o instrumento de notificação eletrónico desenvolvido e gerido pela Comissão que contém uma lista de todos os organismos notificados.

(52) Como os organismos notificados podem propor os seus serviços em todo o território da União, é conveniente dar aos outros Estados-Membros e à Comissão a oportunidade de formular objeções em relação a um organismo notificado. Assim, é primordial prever um período durante o qual possam ser esclarecidas quaisquer dúvidas ou preocupações quanto à competência dos organismos de avaliação da conformidade antes que estes iniciem a suas funções como organismos notificados.

(53) No interesse da competitividade, é crucial que os organismos notificados apliquem os procedimentos de avaliação da conformidade sem sobrecarregar desnecessariamente os operadores económicos. Pelo mesmo motivo, e para favorecer a igualdade de tratamento dos operadores económicos, é necessário assegurar que a aplicação técnica dos procedimentos de avaliação da conformidade seja feita de forma coerente. A melhor maneira de o conseguir é através de uma coordenação e cooperação adequadas entre os organismos notificados.

(54) A fiscalização do mercado é um instrumento essencial para garantir a aplicação correta e uniforme da legislação da União. Convém, pois, criar um quadro jurídico no âmbito do qual a fiscalização do mercado possa ser realizada de forma adequada. As regras relativas à fiscalização do mercado da União e ao controlo dos produtos que entram no mercado da União, previstas no Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho[20], aplicam-se aos produtos com elementos digitais abrangidos pelo presente regulamento.

[20] Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos e que altera a Diretiva 2004/42/CE e os Regulamentos (CE) n.º 765/2008 e (UE) n.º 305/2011 (JO L 169 de 25.6.2019, p. 1).

(55) Em conformidade com o Regulamento (UE) 2019/1020, as autoridades de fiscalização do mercado procedem à fiscalização do mercado no território do respetivo Estado-Membro. O presente regulamento não deve impedir os Estados-Membros de escolher as autoridades competentes para desempenhar essas funções. Cada Estado-Membro deve designar uma ou mais autoridades de fiscalização do mercado no seu território. Os Estados-Membros podem optar por designar qualquer autoridade existente ou nova para atuar como autoridade de fiscalização do mercado, incluindo as autoridades nacionais competentes referidas no artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)] ou as autoridades nacionais de certificação da cibersegurança designadas a que se refere o artigo 58.º do Regulamento (UE) 2019/881. Os operadores económicos devem cooperar plenamente com as autoridades de fiscalização do mercado e outras autoridades competentes. Cada Estado-Membro deve informar a Comissão e os outros Estados-Membros sobre as suas autoridades de fiscalização do mercado e respetivos domínios de competência e deve assegurar os recursos e competências necessários ao desempenho das funções de fiscalização relacionadas com o presente regulamento. Em conformidade com o artigo 10.º, n.os 2 e 3, do Regulamento (UE) 2019/1020, cada Estado-Membro deve designar um serviço de ligação único responsável, nomeadamente, pela representação da posição coordenada das autoridades de fiscalização do mercado e pela assistência na cooperação entre as autoridades de fiscalização do mercado nos diferentes Estados-Membros.

(56) Deve ser criado um grupo de cooperação administrativa (ADCO) específico para a aplicação uniforme do presente regulamento, nos termos do artigo 30.º, n.º 2, do Regulamento (UE) 2019/1020. Este grupo ADCO deve incluir representantes das autoridades de fiscalização do mercado designadas e, se for caso disso, representantes dos serviços de ligação únicos. A Comissão deve apoiar e incentivar a cooperação entre as autoridades de fiscalização do mercado através da rede da União para a conformidade dos produtos, criada com base no artigo 29.º do Regulamento (UE) 2019/1020 e composta por representantes de cada Estado-Membro, incluindo um representante de cada serviço de ligação único a que refere o artigo 10.º do Regulamento (UE) 2019/1020, e um perito nacional facultativo, os presidentes dos ADCO e representantes da Comissão. A Comissão deve participar nas reuniões da rede, dos seus subgrupos e do respetivo ADCO. Deve igualmente prestar assistência a este ADCO através de um secretariado executivo que faculte apoio técnico e logístico.

(57) A fim de assegurar medidas oportunas, proporcionadas e eficazes em relação a produtos com elementos digitais que apresentem um risco de cibersegurança significativo, deve prever-se um procedimento de salvaguarda da União no âmbito do qual as partes interessadas sejam informadas das medidas previstas para esses produtos. Tal deve ainda permitir às autoridades de fiscalização do mercado atuar numa fase precoce, se necessário, em cooperação com os operadores económicos pertinentes. Nos casos em que os Estados-Membros e a Comissão concordem quanto à justificação de uma medida tomada por um Estado-Membro, não deve ser necessária qualquer outra intervenção da Comissão, salvo se a não conformidade puder ser imputada a deficiências de uma norma harmonizada.

(58) Em certos casos, um produto com elementos digitais que cumpra o disposto no presente regulamento pode, não obstante, apresentar um risco de cibersegurança significativo ou constituir um risco para a saúde ou a segurança das pessoas, para o cumprimento de obrigações ao abrigo do direito da União ou do direito nacional destinadas a proteger os direitos fundamentais, a disponibilidade, autenticidade,

integridade ou confidencialidade dos serviços oferecidos através de um sistema de informação eletrónico por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)] ou para outros aspetos da proteção do interesse público. Por conseguinte, é necessário estabelecer regras que assegurem a atenuação desses riscos. Consequentemente, as autoridades de fiscalização do mercado devem tomar medidas para exigir que o operador económico assegure que o produto deixe de apresentar esse risco, que o recolha ou que o retire do mercado, consoante o risco. Assim que uma autoridade de fiscalização do mercado restrinja ou proíba a livre circulação de um produto dessa forma, o Estado-Membro deve notificar as medidas provisórias sem demora à Comissão e aos outros Estados-Membros, justificando e fundamentando a sua decisão. Sempre que uma autoridade de fiscalização do mercado adote tais medidas contra produtos que apresentem um risco, a Comissão deve iniciar consultas com os Estados-Membros e o(s) operador(es) económico(s) em causa e avaliar a medida nacional. Com base nos resultados desta avaliação, a Comissão deve decidir se a medida nacional é ou não justificada. Os Estados-Membros são os destinatários dessa decisão, que lhes é imediatamente comunicada pela Comissão, bem como ao(s) operador(es) económico(s) em causa. Se se considerar que a medida é justificada, a Comissão pode igualmente ponderar a adoção de propostas de revisão da legislação da União aplicável.

(59) No caso de produtos com elementos digitais que apresentem um risco de cibersegurança significativo, e sempre que existam motivos para crer que não são conformes com o presente regulamento, ou de produtos que estão em conformidade com o presente regulamento, mas que apresentam outros riscos importantes, tais como riscos para a saúde ou a segurança das pessoas, para os direitos fundamentais ou para a prestação de serviços por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)], a Comissão pode solicitar à ENISA que realize uma avaliação. Com base nessa avaliação, a Comissão pode adotar, através de atos de execução, medidas corretivas ou restritivas a nível da União, nomeadamente ordenando a retirada do mercado ou a recolha dos produtos correspondentes, num prazo razoável e proporcional à natureza do risco. A Comissão só pode recorrer a essa intervenção em circunstâncias excecionais que justifiquem uma intervenção imediata para preservar o bom funcionamento do mercado interno, e apenas se as autoridades de fiscalização não tiverem tomado medidas eficazes para corrigir a situação. Essas circunstâncias excecionais podem corresponder a situações de emergência em que, por exemplo, um produto não conforme seja generalizadamente disponibilizado pelo fabricante em vários Estados-Membros e também utilizado em setores fundamentais por entidades abrangidas pelo âmbito de aplicação da [Diretiva XXX/XXXX (SRI 2)], embora contenha vulnerabilidades conhecidas que estão a ser exploradas por agentes mal-intencionados e para as quais o fabricante não faculte atualizações corretivas. A Comissão pode intervir nessas situações de emergência apenas enquanto as circunstâncias excecionais se verificarem e se o incumprimento do presente regulamento ou os riscos importantes detetados persistirem.

(60) Nos casos em que existam indícios de incumprimento do presente regulamento em vários Estados-Membros, as autoridades de fiscalização do mercado devem poder realizar atividades conjuntas com outras autoridades, com vista a verificar a conformidade e identificar os riscos de cibersegurança dos produtos com elementos digitais.

(61) As ações de controlo coordenadas simultâneas (ações de fiscalização conjuntas ou «sweeps») são ações de execução específicas das autoridades de fiscalização do

mercado que podem reforçar ainda mais a segurança dos produtos. Em especial, devem ser realizadas ações de fiscalização conjuntas sempre que as tendências do mercado, as queixas dos consumidores ou outros indícios sugiram que determinadas categorias de produtos apresentam frequentemente riscos de cibersegurança. A ENISA deve apresentar às autoridades de fiscalização do mercado propostas de categorias de produtos para as quais poderão ser organizadas ações de fiscalização conjuntas, com base, nomeadamente, nas notificações de vulnerabilidades de produtos e incidentes que recebe.

(62) A fim de assegurar que o quadro regulamentar possa ser adaptado sempre que necessário, deve ser delegado na Comissão o poder de adotar atos nos termos do artigo 290.º do Tratado no que diz respeito à atualização da lista de produtos críticos constante do anexo III e à especificação das definições destas categorias de produtos. Deve ser delegado na Comissão o poder de adotar atos nos termos desse artigo a fim de identificar os produtos com elementos digitais abrangidos por outras regras da União que permitam alcançar o mesmo nível de proteção que o presente regulamento, especificando se será necessária uma limitação ou exclusão do âmbito de aplicação do presente regulamento, bem como o âmbito dessa limitação, se for caso disso. Deve também ser delegado na Comissão o poder de adotar atos nos termos desse artigo no que diz respeito à potencial obrigatoriedade de certificação de determinados produtos altamente críticos com elementos digitais com base nos critérios de criticidade estabelecidos no presente regulamento, bem como para especificar o conteúdo mínimo da declaração de conformidade UE e complementar os elementos a incluir na documentação técnica. É particularmente importante que a Comissão proceda a consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[21]. Em especial, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados- Membros e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratam da preparação dos atos delegados.

(63) A fim de assegurar condições uniformes para a execução do presente regulamento, devem ser atribuídas competências de execução à Comissão para: especificar o formato e os elementos da lista de materiais do *software*, especificar mais pormenorizadamente o tipo de informações, o formato e o procedimento das notificações de vulnerabilidades ativamente exploradas e incidentes apresentadas à ENISA pelos fabricantes, especificar os sistemas europeus de certificação da cibersegurança adotados nos termos do Regulamento (UE) 2019/881 que podem ser utilizados para demonstrar a conformidade com os requisitos essenciais, ou partes dos mesmos, estabelecidos no anexo I do presente regulamento, adotar especificações comuns no que respeita aos requisitos essenciais estabelecidos no anexo I, estabelecer especificações técnicas para os pictogramas ou quaisquer outras marcas relacionadas com a segurança dos produtos com elementos digitais, bem como mecanismos para promover a sua utilização, e decidir sobre medidas corretivas ou restritivas a nível da União em circunstâncias excecionais que justifiquem uma intervenção imediata para preservar o bom funcionamento do mercado interno. Tais competências devem ser

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

exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[22].

(64) Para assegurar uma cooperação de confiança e construtiva entre as autoridades de fiscalização do mercado a nível da União e a nível nacional, todas as partes envolvidas na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções.

(65) A fim de assegurar a aplicação efetiva das obrigações estabelecidas no presente regulamento, cada autoridade de fiscalização do mercado deve ter poderes para impor ou solicitar a imposição de coimas. Por conseguinte, devem ser fixados os níveis máximos das coimas a prever na legislação nacional pelo incumprimento das obrigações estabelecidas no presente regulamento. Ao decidir sobre o montante da coima aplicável a cada caso individual, devem ser tidas em conta todas as circunstâncias pertinentes da situação específica e, no mínimo, as explicitamente estabelecidas no presente regulamento, inclusive se já foram aplicadas coimas por outras autoridades de fiscalização do mercado ao mesmo operador por infrações semelhantes. As referidas circunstâncias podem ser agravantes, em situações em que a infração cometida pelo mesmo operador persista no território de outros Estados-Membros que não aquele em que já foi aplicada uma coima, ou atenuantes, para garantir que qualquer outra coima considerada por outra autoridade de fiscalização do mercado para o mesmo operador económico ou para o mesmo tipo de infração já tenha em conta, juntamente com outras circunstâncias específicas pertinentes, uma sanção e o seu montante impostos noutros Estados-Membros. Em todos esses casos, a coima cumulativa que poderá ser aplicada pelas autoridades de fiscalização do mercado de vários Estados-Membros ao mesmo operador económico pelo mesmo tipo de infração deve assegurar o respeito do princípio da proporcionalidade.

(66) Sempre que forem impostas coimas a pessoas que não sejam empresas, a autoridade competente deve ter em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em causa, no momento de estabelecer o montante adequado da coima. Deve caber aos Estados-Membros determinar se as autoridades públicas devem estar sujeitas a coimas, e em que medida.

(67) Nas suas relações com países terceiros, a UE esforça-se por promover o comércio internacional dos produtos regulamentados. Pode ser aplicada uma grande variedade de medidas para promover o comércio, incluindo vários instrumentos jurídicos, como os acordos bilaterais (intergovernamentais) de reconhecimento mútuo (ARM) para a avaliação da conformidade e a marcação de produtos regulamentados. Os ARM são celebrados entre a União e os países terceiros que beneficiem de um nível de desenvolvimento técnico comparável e prossigam uma abordagem compatível em matéria de avaliação da conformidade. Estes acordos baseiam-se na aceitação mútua de certificados, marcas de conformidade e relatórios de ensaio emitidos pelos organismos de avaliação da conformidade de qualquer uma das partes, em conformidade com a legislação da outra parte. Estão atualmente em vigor ARM com vários países. Estes acordos são celebrados numa série de setores específicos, que podem variar de um país para outro. A fim de facilitar ainda mais o comércio, e reconhecendo que as cadeias de abastecimento de produtos com elementos digitais são

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

globais, a União pode celebrar ARM relativos à avaliação da conformidade para os produtos regidos pelo presente regulamento, em conformidade com o artigo 218.º do TFUE. A cooperação com países parceiros também é importante para reforçar a ciber-resiliência a nível mundial, uma vez que, a longo prazo, contribuirá para um quadro de cibersegurança robustecido, tanto dentro como fora da UE.

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

(69) Os operadores económicos devem dispor de tempo suficiente para se adaptarem aos requisitos do presente regulamento. O presente regulamento deve ser aplicável [24 meses] após a sua entrada em vigor, com exceção das obrigações de comunicação de vulnerabilidades ativamente exploradas e incidentes, que devem ser aplicáveis [12 meses] após a data de entrada em vigor do presente regulamento.

(70) Atendendo a que o objetivo do presente regulamento não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

(71) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[23] e emitiu o seu parecer em […],

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento estabelece o seguinte:

(a) Regras para a colocação no mercado de produtos com elementos digitais, a fim de garantir a cibersegurança desses produtos;

(b) Requisitos essenciais para a conceção, o desenvolvimento e a produção de produtos com elementos digitais e as obrigações dos operadores económicos em relação a esses produtos no que diz respeito à cibersegurança;

(c) Requisitos essenciais para os processos de tratamento de vulnerabilidades aplicados pelos fabricantes de modo a garantir a cibersegurança dos produtos com elementos

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

digitais durante todo o ciclo de vida, bem como as obrigações dos operadores económicos em relação a esses processos;

(d) Regras relativas à fiscalização do mercado e à aplicação das regras e dos requisitos referidos acima.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento é aplicável aos produtos com elementos digitais cuja utilização prevista ou razoavelmente previsível inclua uma conexão de dados lógica ou física, direta ou indireta, a um dispositivo ou a uma rede.

2. O presente regulamento não é aplicável aos produtos com elementos digitais aos quais sejam aplicáveis os seguintes atos da União:

   (a) Regulamento (UE) 2017/745;

   (b) Regulamento (UE) 2017/746;

   (c) Regulamento (UE) 2019/2144.

3. O presente regulamento não é aplicável aos produtos com elementos digitais que tenham sido certificados nos termos do Regulamento (UE) 2018/1139.

4. A aplicação do presente regulamento aos produtos com elementos digitais abrangidos por outras regras da União que estabeleçam requisitos que deem resposta à totalidade ou a parte dos riscos abrangidos pelos requisitos essenciais constantes do anexo I pode ser limitada ou excluída, se:

   (a) Tal limitação ou exclusão for congruente com o quadro regulamentar global aplicável a esses produtos; e

   (b) As regras setoriais permitirem alcançar o mesmo nível de proteção que o previsto no presente regulamento.

   A Comissão fica habilitada a adotar atos delegados nos termos do artigo 50.º de forma a alterar o presente regulamento, especificando se tal limitação ou exclusão é necessária, os produtos e as regras em causa, bem como o âmbito da limitação, se for caso disso.

5. O presente regulamento não é aplicável a produtos com elementos digitais desenvolvidos exclusivamente para fins militares ou de segurança nacional, nem a produtos especificamente concebidos para o tratamento de informações classificadas.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Produto com elementos digitais», qualquer produto de *software* ou *hardware* e as suas soluções de tratamento remoto de dados, incluindo componentes de *software* ou *hardware* a colocar no mercado separadamente;

(2) «Tratamento remoto de dados», qualquer tratamento de dados à distância para o qual o *software* tenha sido concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade e cuja inexistência impediria o produto com elementos digitais de desempenhar uma das suas funções;

(3) «Produto crítico com elementos digitais», um produto com elementos digitais que apresente um risco de cibersegurança em conformidade com os critérios estabelecidos no artigo 6.º, n.º 2, e cuja funcionalidade principal conste do anexo III;

(4) «Produto altamente crítico com elementos digitais», um produto com elementos digitais que apresente um risco de cibersegurança em conformidade com os critérios estabelecidos no artigo 6.º, n.º 5;

(5) «Tecnologia operacional», dispositivos ou sistemas digitais programáveis que interagem com o ambiente físico ou que gerem dispositivos que interagem com o ambiente físico;

(6) «*Software*», a parte de um sistema de informação eletrónico que consiste em código de computador;

(7) «*Hardware*», um sistema de informação eletrónico físico, ou partes do mesmo, capaz de tratar, armazenar ou transmitir dados digitais;

(8) «Componente», *software* ou *hardware* destinado a ser integrado num sistema de informação eletrónico;

(9) «Sistema de informação eletrónico», qualquer sistema, incluindo equipamento elétrico ou eletrónico, capaz de tratar, armazenar ou transmitir dados digitais;

(10) «Conexão lógica», uma representação virtual de uma conexão de dados efetuada através de uma interface de *software*;

(11) «Conexão física», qualquer conexão entre sistemas de informação eletrónicos ou componentes efetuada por meios físicos, nomeadamente através de interfaces elétricas ou mecânicas, cabos ou ondas radioelétricas;

(12) «Conexão indireta», uma conexão a um dispositivo ou a uma rede que não ocorre diretamente, mas sim como parte de um sistema maior diretamente conectável a esse dispositivo ou rede;

(13) «Privilégio», um direito de acesso concedido a determinados utilizadores ou programas para realizar operações relevantes em termos de segurança num sistema de informação eletrónico;

(14) «Privilégio elevado», um direito de acesso concedido a determinados utilizadores ou programas para realizar um conjunto alargado de operações relevantes em termos de segurança num sistema de informação eletrónico que, caso seja utilizado indevidamente ou fique comprometido, pode permitir a um agente mal-intencionado obter um acesso mais amplo aos recursos de um sistema ou organização;

(15) «Ponto terminal», qualquer dispositivo conectado a uma rede e que serve de ponto de entrada nessa rede;

(16) «Recursos informáticos ou de rede», os dados ou a funcionalidade do *hardware* ou do *software* acessíveis localmente ou através de uma rede ou de outro dispositivo conectado;

(17) «Operador económico», o fabricante, o mandatário, o importador, o distribuidor ou qualquer outra pessoa singular ou coletiva sujeita às obrigações estabelecidas no presente regulamento;

(18) «Fabricante», qualquer pessoa singular ou coletiva que desenvolva ou fabrique produtos com elementos digitais, ou que os mande conceber, desenvolver ou

fabricar, e os comercialize em seu nome ou sob a sua marca, a título oneroso ou gratuito;

(19) «Mandatário», uma pessoa singular ou coletiva, estabelecida na União, mandatada por escrito pelo fabricante para praticar determinados atos em seu nome;

(20) «Importador», uma pessoa singular ou coletiva estabelecida na União que coloque no mercado um produto com elementos digitais que ostente o nome ou a marca de uma pessoa singular ou coletiva estabelecida fora da União;

(21) «Distribuidor», uma pessoa singular ou coletiva inserida na cadeia de abastecimento, distinta do fabricante e do importador, que disponibiliza um produto com elementos digitais no mercado da União sem alterar as suas propriedades;

(22) «Colocação no mercado», a primeira disponibilização de um produto com elementos digitais no mercado da União;

(23) «Disponibilização no mercado», qualquer oferta de um produto com elementos digitais para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial, a título oneroso ou gratuito;

(24) «Finalidade prevista», a utilização à qual o fabricante destina o produto com elementos digitais, incluindo o contexto específico e as condições de utilização, conforme especificada nas informações facultadas pelo fabricante nas instruções de utilização, nos materiais e declarações promocionais ou de venda, bem como na documentação técnica;

(25) «Utilização razoavelmente previsível», utilização que não é necessariamente a finalidade prevista indicada pelo fabricante nas instruções de utilização, nos materiais e declarações promocionais ou de venda, bem como na documentação técnica, mas que pode resultar de comportamentos humanos ou de operações ou interações técnicas razoavelmente previsíveis;

(26) «Utilização indevida razoavelmente previsível», a utilização de um produto com elementos digitais de uma forma não conforme com a sua finalidade prevista, mas que pode resultar de comportamentos humanos ou de interações com outros sistemas razoavelmente previsíveis;

(27) «Autoridade notificadora», a autoridade nacional responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação de organismos de avaliação da conformidade e pelo controlo destes;

(28) «Avaliação da conformidade», o processo de verificação do cumprimento dos requisitos essenciais constantes do anexo I;

(29) «Organismo de avaliação da conformidade», um organismo na aceção do artigo 2.º, ponto 13, do Regulamento (UE) n.º 765/2008;

(30) «Organismo notificado», um organismo de avaliação da conformidade designado nos termos do artigo 33.º do presente regulamento ou de outra legislação de harmonização da União aplicável;

(31) «Modificação substancial», uma alteração do produto com elementos digitais após a sua colocação no mercado que afete a conformidade do produto com elementos digitais com os requisitos essenciais constantes do anexo I, secção 1, ou que resulte numa modificação da utilização prevista para a qual o produto com elementos digitais foi avaliado;

(32) «Marcação CE», a marcação através da qual um fabricante indica que um produto com elementos digitais e os processos por si aplicados estão em conformidade com os requisitos essenciais constantes do anexo I e de outra legislação da União aplicável que harmonize as condições de comercialização dos produtos («legislação de harmonização da União») e preveja a sua aposição;

(33) «Autoridade de fiscalização do mercado», a autoridade de fiscalização do mercado na aceção do artigo 3.º, ponto 4, do Regulamento (UE) 2019/1020;

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

(35) «Risco de cibersegurança», um risco na aceção do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)];

(36) «Risco de cibersegurança significativo», um risco de cibersegurança que, com base nas suas características técnicas, se possa considerar altamente suscetível de dar origem a um incidente com impacto negativo grave, causando, nomeadamente, perturbações ou perdas materiais ou imateriais consideráveis;

(37) «Lista de materiais do *software*», um registo formal que contém informações pormenorizadas e as relações na cadeia de abastecimento dos componentes incluídos nos elementos de *software* de um produto com elementos digitais;

(38) «Vulnerabilidade», uma vulnerabilidade na aceção do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)];

(39) «Vulnerabilidade ativamente explorada», uma vulnerabilidade relativamente à qual existem provas fiáveis da execução de código malicioso num sistema por parte de um agente sem a autorização do proprietário do sistema;

(40) «Dados pessoais», dados pessoais na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679.

Artigo 4.º

Livre circulação

1. Os Estados-Membros não podem dificultar, nas matérias abrangidas pelo presente regulamento, a disponibilização no mercado de produtos com elementos digitais que cumpram o disposto no presente regulamento.

2. Em feiras comerciais, exposições e demonstrações ou eventos semelhantes, os Estados-Membros não podem impedir a apresentação e utilização de um produto com elementos digitais que não cumpra o disposto no presente regulamento.

3. Os Estados-Membros não podem impedir a disponibilização de *software* inacabado que não cumpra o disposto no presente regulamento, contanto que o *software* só seja disponibilizado por um período limitado necessário para efeitos de ensaio e um sinal visível indique nitidamente que não cumpre o disposto no presente regulamento e que não estará disponível no mercado para outros fins que não para fins de ensaio.

Artigo 5.º

Requisitos aplicáveis aos produtos com elementos digitais

Os produtos com elementos digitais só podem ser disponibilizados no mercado se:

(1) Cumprirem os requisitos essenciais constantes do anexo I, secção 1, na condição de serem corretamente instalados, mantidos, utilizados para a respetiva finalidade prevista ou em condições razoavelmente previsíveis e, se for caso disso, atualizados; e

(2) Os processos aplicados pelo fabricante cumprirem os requisitos essenciais constantes do anexo I, secção 2.

Artigo 6.º

Produtos críticos com elementos digitais

1. Os produtos com elementos digitais pertencentes a uma categoria enumerada no anexo III são considerados produtos críticos com elementos digitais. Considera-se que são abrangidos por uma das categorias enumeradas no anexo III do presente regulamento os produtos que tenham a funcionalidade principal dessa categoria. As categorias de produtos críticos com elementos digitais dividem-se nas classes I e II, tal como estabelecido no anexo III, refletindo o nível de risco de cibersegurança associado a esses produtos.

2. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 50.º para alterar o anexo III incluindo na lista de categorias de produtos críticos com elementos digitais uma nova categoria ou retirando uma categoria existente. Ao avaliar a necessidade de alterar a lista constante do anexo III, a Comissão deve ter em conta o nível de risco de cibersegurança associado à categoria de produtos com elementos digitais. Para determinar o nível de risco de cibersegurança, devem ser tidos em conta um ou vários dos seguintes critérios:

   (a) A funcionalidade relacionada com a cibersegurança do produto com elementos digitais e o facto de este ter, pelo menos, um dos seguintes atributos:

      (i) foi concebido para funcionar com privilégios elevados ou para gerir privilégios,

      (ii) tem acesso direto ou privilegiado a recursos informáticos ou de rede,

      (iii) foi concebido para controlar o acesso aos dados ou à tecnologia operacional,

      (iv) desempenha uma função essencial para a confiança, em especial funções de segurança como o controlo da rede, a segurança de pontos terminais e a proteção da rede;

   (b) A utilização prevista em ambientes sensíveis, incluindo em contextos industriais ou por entidades essenciais do tipo referido no anexo [anexo I] da Diretiva [Diretiva XXX/XXXX (SRI 2)];

   (c) O fim previsto de execução de funções críticas ou sensíveis, como o tratamento de dados pessoais;

   (d) O potencial alcance de um impacto adverso, nomeadamente em termos de intensidade e de capacidade para afetar um grande número de pessoas;

(e) A medida em que a utilização de produtos com elementos digitais já causou perturbações ou perdas materiais ou imateriais, ou suscitou preocupações significativas em relação à materialização de um impacto adverso.

3. A Comissão fica habilitada a adotar um ato delegado nos termos do artigo 50.º para completar o presente regulamento especificando as definições das categorias de produtos das classes I e II constantes do anexo III. O ato delegado deve ser adotado [até 12 meses após a entrada em vigor do presente regulamento].

4. Os produtos críticos com elementos digitais ficam sujeitos aos procedimentos de avaliação da conformidade referidos no artigo 24.º, n.os 2 e 3.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 50.º para completar o presente regulamento especificando as categorias de produtos altamente críticos com elementos digitais para as quais se exige que os fabricantes obtenham um certificado europeu de cibersegurança ao abrigo de um sistema europeu de certificação da cibersegurança nos termos do Regulamento (UE) 2019/881, de modo a demonstrar a conformidade com os requisitos essenciais constantes do anexo I, ou partes dos mesmos. Ao determinar tais categorias de produtos altamente críticos com elementos digitais, a Comissão deve ter em conta o nível de risco de cibersegurança associado à categoria de produtos com elementos digitais, à luz de um ou vários critérios enumerados no n.º 2, bem como de uma avaliação que indique se a categoria de produtos:

(a) É utilizada ou serve de base a entidades essenciais do tipo referido no anexo [anexo I] da Diretiva [Diretiva XXX/XXXX (SRI 2)] ou é suscetível de ter importância no futuro para as atividades destas entidades; ou

(b) É relevante para a resiliência da cadeia de abastecimento global dos produtos com elementos digitais face a acontecimentos disruptivos.

Artigo 7.º

Segurança geral dos produtos

Em derrogação do artigo 2.º, n.º 1, terceiro parágrafo, alínea b), do Regulamento [Regulamento Segurança Geral dos Produtos], sempre que os produtos com elementos digitais não estejam sujeitos a requisitos específicos estabelecidos noutra legislação de harmonização da União na aceção do [artigo 3.º, n.º 25, do Regulamento Segurança Geral dos Produtos], aplicam-se a esses produtos o capítulo III, secção 1, os capítulos V e VII e os capítulos IX a XI do Regulamento [Regulamento Segurança Geral dos Produtos] no que respeita aos riscos de segurança não abrangidos pelo presente regulamento.

Artigo 8.º

Sistemas de IA de risco elevado

1. Os produtos com elementos digitais classificados como sistemas de IA de risco elevado nos termos do artigo [artigo 6.º] do Regulamento [Regulamento Inteligência Artificial] que sejam abrangidos pelo âmbito de aplicação do presente regulamento e cumpram os requisitos essenciais constantes do anexo I, secção 1, do presente regulamento, e cujos processos aplicados pelo fabricante estejam em conformidade com os requisitos essenciais constantes do anexo I, secção 2, são considerados conformes com os requisitos de cibersegurança estabelecidos no artigo [artigo 15.º] do Regulamento [Regulamento Inteligência Artificial], sem prejuízo dos demais

requisitos de exatidão e solidez previstos no referido artigo, e na medida em que a consecução do nível de proteção exigido por esses requisitos seja demonstrada pela declaração de conformidade UE emitida ao abrigo do presente regulamento.

2. Os produtos e os requisitos de cibersegurança referidos no n.º 1 estão sujeitos ao procedimento de avaliação da conformidade pertinente exigido pelo artigo [artigo 43.º] do Regulamento [Regulamento Inteligência Artificial]. Para efeitos dessa avaliação, os organismos notificados habilitados a verificar a conformidade dos sistemas de IA de risco elevado ao abrigo do [Regulamento Inteligência Artificial] ficam igualmente habilitados a verificar a conformidade dos sistemas de IA de risco elevado abrangidos pelo âmbito de aplicação do presente regulamento com os requisitos constantes do anexo I do presente regulamento, contanto que a conformidade desses organismos notificados com os requisitos estabelecidos no artigo 29.º do presente regulamento tenha sido avaliada no contexto do procedimento de notificação previsto no Regulamento [Regulamento Inteligência Artificial].

3. Em derrogação do n.º 2, os produtos críticos com elementos digitais enumerados no anexo III do presente regulamento que tenham de aplicar os procedimentos de avaliação da conformidade referidos no artigo 24.º, n.º 2, alíneas a) e b), e no artigo 24.º, n.º 3, alíneas a) e b), do presente regulamento, que sejam igualmente classificados como sistemas de IA de risco elevado nos termos do artigo [artigo 6.º] do Regulamento [Regulamento Inteligência Artificial] e aos quais seja aplicável o procedimento de avaliação da conformidade baseado no controlo interno referido no anexo [anexo VI] do Regulamento [Regulamento Inteligência Artificial], ficam sujeitos aos procedimentos de avaliação da conformidade exigidos pelo presente regulamento no que diz respeito aos requisitos essenciais nele previstos.

Artigo 9.º

Máquinas e seus componentes e acessórios

As máquinas e seus componentes e acessórios abrangidos pelo âmbito de aplicação do Regulamento [proposta de Regulamento Máquinas] que sejam produtos com elementos digitais na aceção do presente regulamento e para os quais tenha sido emitida uma declaração de conformidade UE com base no presente regulamento são considerados conformes com os requisitos essenciais de saúde e segurança constantes do anexo [anexo III, pontos 1.1.9 e 1.2.1] do Regulamento [proposta de Regulamento Máquinas], no que concerne à proteção contra a corrupção e à segurança e fiabilidade dos sistemas de comando, na medida em que a consecução do nível de proteção exigido por esses requisitos seja demonstrada na declaração de conformidade UE emitida ao abrigo do presente regulamento.

CAPÍTULO II

OBRIGAÇÕES DOS OPERADORES ECONÓMICOS

Artigo 10.º

Obrigações dos fabricantes

1. Quando colocam um produto com elementos digitais no mercado, os fabricantes devem assegurar que esse produto foi concebido, desenvolvido e produzido em conformidade com os requisitos essenciais constantes do anexo I, secção 1.

2. Para efeitos do cumprimento da obrigação estabelecida no n.º 1, os fabricantes devem efetuar uma avaliação dos riscos de cibersegurança associados a um produto com elementos digitais e ter em conta o resultado dessa avaliação durante as fases de planeamento, conceção, desenvolvimento, produção, entrega e manutenção do produto com elementos digitais, com vista a minimizar os riscos de cibersegurança, prevenir incidentes de segurança e minimizar os impactos de tais incidentes, nomeadamente na saúde e segurança dos utilizadores.

3. Ao colocar um produto com elementos digitais no mercado, o fabricante deve incluir uma avaliação dos riscos de cibersegurança na documentação técnica prevista no artigo 23.º no anexo V. Para os produtos com elementos digitais referidos no artigo 8.º e no artigo 24.º, n.º 4, que também sejam abrangidos por outros atos da União, a avaliação dos riscos de cibersegurança pode integrar a avaliação dos riscos exigida pelos respetivos atos da União. Sempre que determinados requisitos essenciais não sejam aplicáveis ao produto com elementos digitais comercializado, o fabricante deve incluir uma justificação clara na referida documentação.

4. Para efeitos do cumprimento da obrigação estabelecida no n.º 1, os fabricantes devem exercer a diligência devida quando integram componentes provenientes de terceiros em produtos com elementos digitais. Cabe aos fabricantes assegurar que esses componentes não comprometem a segurança do produto com elementos digitais.

5. O fabricante deve documentar sistematicamente os aspetos de cibersegurança pertinentes respeitantes ao produto com elementos digitais, de forma proporcional à sua natureza e aos riscos de cibersegurança, incluindo as vulnerabilidades de que tenha conhecimento e eventuais informações pertinentes comunicadas por terceiros, bem como, se for caso disso, atualizar a avaliação dos riscos do produto.

6. Ao colocarem um produto com elementos digitais no mercado e durante o tempo de vida esperado do produto ou por um período de cinco anos a contar da data da sua colocação no mercado, consoante o que for mais breve, os fabricantes devem assegurar que as vulnerabilidades desse produto são tratadas de forma eficaz e em conformidade com os requisitos essenciais constantes do anexo I, secção 2.

   Os fabricantes devem dispor de políticas e procedimentos adequados, incluindo as políticas de divulgação coordenada de vulnerabilidades referidas no anexo I, secção 2, ponto 5, para tratar e corrigir potenciais vulnerabilidades no produto com elementos digitais comunicadas por fontes internas ou externas.

7. Antes de colocarem um produto com elementos digitais no mercado, os fabricantes devem elaborar a documentação técnica referida no artigo 23.º.

   Os fabricantes devem executar ou mandar executar os procedimentos de avaliação da conformidade escolhidos referidos no artigo 24.º.

   Sempre que a conformidade do produto com elementos digitais com os requisitos essenciais constantes do anexo I, secção 1, e dos processos aplicados pelo fabricante com os requisitos essenciais constantes do anexo I, secção 2, tenha sido demonstrada através desse procedimento de avaliação da conformidade, os fabricantes devem elaborar a declaração de conformidade UE nos termos do artigo 20.º e apor a marcação CE nos termos do artigo 22.º.

8. Os fabricantes devem manter a documentação técnica e a declaração de conformidade UE, quando pertinente, à disposição das autoridades de fiscalização do

mercado por um período de dez anos a contar da data de colocação no mercado do produto com elementos digitais.

9. Os fabricantes devem assegurar a existência de procedimentos para manter a conformidade dos produtos com elementos digitais que façam parte de uma produção em série. O fabricante deve ter devidamente em conta as alterações dos processos de produção e desenvolvimento ou da conceção ou características do produto com elementos digitais, bem como as alterações das normas harmonizadas, dos sistemas europeus de certificação da cibersegurança ou das especificações comuns referidas no artigo 19.º que constituíram a referência para a declaração ou para a verificação da conformidade do produto com elementos digitais.

10. Cabe aos fabricantes assegurar que os produtos com elementos digitais são acompanhados das informações e instruções previstas no anexo II, em formato eletrónico ou físico. Tais informações e instruções devem ser redigidas numa língua que possa ser facilmente compreendida pelos utilizadores. Devem ser claras, compreensíveis, inteligíveis e legíveis. Devem permitir a instalação, o funcionamento e a utilização seguros dos produtos com elementos digitais.

11. Os fabricantes devem fornecer a declaração de conformidade UE juntamente com o produto com elementos digitais ou devem incluir nas instruções e informações previstas no anexo II o endereço Internet em que tal declaração de conformidade UE pode ser consultada.

12. A partir da colocação do produto com elementos digitais no mercado e durante o seu tempo de vida esperado ou por um período de cinco anos a contar da sua data de colocação no mercado, consoante o que for mais breve, os fabricantes que saibam ou tenham motivos para crer que o produto com elementos digitais ou os processos por si aplicados não estão em conformidade com os requisitos essenciais constantes do anexo I devem tomar imediatamente as medidas corretivas necessárias para assegurar a conformidade do produto com elementos digitais ou dos seus processos, para retirar esse produto ou para o recolher, consoante o caso.

13. Mediante pedido fundamentado de uma autoridade de fiscalização do mercado, os fabricantes devem facultar à referida autoridade, numa língua que possa ser facilmente compreendida, todas as informações e documentação, em papel ou em suporte eletrónico, necessárias para demonstrar a conformidade do produto com elementos digitais e dos processos aplicados pelo fabricante com os requisitos essenciais constantes do anexo I. Os fabricantes devem cooperar com a referida autoridade, a pedido desta, no âmbito de quaisquer medidas tomadas para eliminar os riscos de cibersegurança decorrentes do produto com elementos digitais que tenham colocado no mercado.

14. Os fabricantes que cessem a sua atividade e, por conseguinte, não estejam em condições de cumprir as obrigações estabelecidas no presente regulamento devem informar desse facto, antes de a cessação da atividade produzir efeitos, as autoridades de fiscalização do mercado competentes, bem como os utilizadores dos produtos com elementos digitais em causa colocados no mercado, por todos os meios disponíveis e tanto quanto possível.

15. A Comissão pode especificar, por meio de atos de execução, o formato e os elementos da lista de materiais do *software* previstos no anexo I, secção 2, ponto 1. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

Artigo 11.º

Obrigações dos fabricantes em matéria de comunicação de informações

1. O fabricante deve, sem demora injustificada e, em todo o caso, no prazo de 24 horas após ter tomado conhecimento desse facto, notificar à ENISA qualquer vulnerabilidade ativamente explorada existente no produto com elementos digitais. A notificação deve incluir pormenores sobre a referida vulnerabilidade e, se for caso disso, as medidas corretivas ou de atenuação que tenham sido tomadas. Após a receção, a ENISA deve transmitir a notificação, sem demora injustificada, salvo por motivos fundamentados relacionados com o risco de cibersegurança, à CSIRT dos Estados-Membros em causa designada, para efeitos de divulgação coordenada de vulnerabilidades, nos termos do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)] e informar a autoridade de fiscalização do mercado da vulnerabilidade notificada.

2. O fabricante deve, sem demora injustificada e, em todo o caso, no prazo de 24 horas após ter tomado conhecimento desse facto, notificar à ENISA qualquer incidente que afete a segurança do produto com elementos digitais. A ENISA deve transmitir as notificações, sem demora injustificada, salvo por motivos fundamentados relacionados com o risco de cibersegurança, ao ponto de contacto único dos Estados-Membros em causa designado nos termos do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)] e informar a autoridade de fiscalização do mercado sobre os incidentes notificados. A notificação do incidente deve incluir informações sobre a gravidade e o impacto do incidente e, se for caso disso, deve indicar se o fabricante suspeita que este tenha sido causado por atos ilícitos ou mal-intencionados ou se considera que tenha um impacto transfronteiriço.

3. A ENISA deve apresentar à Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe), criada pelo artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)], informações notificadas nos termos dos n.os 1 e 2 se tais informações forem relevantes para a gestão coordenada de incidentes e crises de cibersegurança em grande escala a um nível operacional.

4. O fabricante deve informar os utilizadores do produto com elementos digitais, sem demora injustificada e após ter tomado conhecimento desse facto, sobre o incidente e, se necessário, sobre as medidas corretivas que o utilizador pode tomar para atenuar o impacto do incidente.

5. A Comissão pode especificar mais aprofundadamente, por meio de atos de execução, o tipo de informações, o formato e o procedimento das notificações apresentadas nos termos dos n.os 1 e 2. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

6. Com base nas notificações recebidas nos termos dos n.os 1 e 2, a ENISA elabora, de dois em dois anos, um relatório técnico sobre as tendências emergentes em matéria de riscos de cibersegurança dos produtos com elementos digitais e apresenta-o ao grupo de cooperação referido no artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)]. O primeiro desses relatórios deve ser apresentado no prazo de 24 meses a contar da data de início da aplicação das obrigações previstas nos n.os 1 e 2.

7. Ao identificarem uma vulnerabilidade num componente, incluindo um componente de código aberto, integrado no produto com elementos digitais, os fabricantes devem comunicar a vulnerabilidade à pessoa ou entidade responsável pela manutenção do componente.

Artigo 12.º

Mandatários

1. Um fabricante pode designar um mandatário por meio de um mandato escrito.

2. Não fazem parte do respetivo mandato as obrigações previstas no artigo 10.º, n.os 1 a 7, primeiro parágrafo, e n.º 9.

3. O mandatário pratica os atos especificados no mandato conferido pelo fabricante. O mandato deve permitir ao mandatário praticar, pelo menos, os seguintes atos:

   (a) Manter à disposição das autoridades de fiscalização do mercado a declaração de conformidade UE referida no artigo 20.º e a documentação técnica referida no artigo 23.º durante dez anos após a data de colocação do produto com elementos digitais no mercado;

   (b) Mediante pedido fundamentado da autoridade de fiscalização do mercado, facultar-lhe toda a informação e a documentação necessárias para demonstrar a conformidade do produto com elementos digitais;

   (c) Cooperar com as autoridades de fiscalização do mercado, a pedido destas, no que se refere a todas as medidas tomadas para eliminar os riscos decorrentes do produto com elementos digitais abrangido pelo seu mandato.

Artigo 13.º

Obrigações dos importadores

1. Os importadores só podem colocar no mercado produtos com elementos digitais que cumpram os requisitos essenciais constantes do anexo I, secção 1, e se os processos aplicados pelo fabricante cumprirem os requisitos essenciais constantes do anexo I, secção 2.

2. Antes de colocarem um produto com elementos digitais no mercado, os importadores devem assegurar que:

   (a) O fabricante aplicou os procedimentos de avaliação da conformidade adequados a que se refere o artigo 24.º;

   (b) O fabricante elaborou a documentação técnica;

   (c) O produto com elementos digitais ostenta a marcação CE referida no artigo 22.º e é acompanhado das informações e instruções de utilização previstas no anexo II.

3. Sempre que considere ou tenha motivos para crer que um produto com elementos digitais ou os processos aplicados pelo fabricante não estão em conformidade com os requisitos essenciais constantes do anexo I, o importador não pode colocar o produto no mercado antes de se assegurar a conformidade desse produto ou dos processos aplicados pelo fabricante com os requisitos essenciais do referido anexo. Além disso, se o produto com elementos digitais apresentar um risco de cibersegurança significativo, o importador deve informar o fabricante e as autoridades de fiscalização do mercado desse facto.

4. Os importadores devem indicar o seu nome, nome comercial registado ou marca registada, o endereço postal e o endereço de correio eletrónico de contacto no produto com elementos digitais ou, se tal não for possível, na embalagem ou num documento que acompanhe o produto com elementos digitais. Os contactos são

apresentados numa língua que possa ser facilmente compreendida pelos utilizadores e pelas autoridades de fiscalização do mercado.

5. Os importadores devem assegurar que o produto com elementos digitais seja acompanhado das instruções e informações previstas no anexo II, numa língua que possa ser facilmente compreendida pelos utilizadores.

6. Os importadores que saibam ou tenham motivos para crer que um produto com elementos digitais que colocaram no mercado, ou os processos aplicados pelo seu fabricante, não estão em conformidade com os requisitos essenciais constantes do anexo I devem tomar imediatamente as medidas corretivas necessárias para assegurar a conformidade dos elementos digitais ou dos processos aplicados pelo seu fabricante com os requisitos essenciais do referido anexo, ou para retirar ou recolher o produto, se for caso disso.

   Ao identificarem uma vulnerabilidade no produto com elementos digitais, os importadores devem informar o fabricante, sem demora injustificada, dessa vulnerabilidade. Além disso, se o produto com elementos digitais apresentar um risco de cibersegurança significativo, os importadores devem informar imediatamente desse facto as autoridades de fiscalização do mercado dos Estados-Membros em cujo mercado disponibilizaram o produto com elementos digitais, fornecendo-lhes as informações relevantes, sobretudo no que se refere à não conformidade e às medidas corretivas aplicadas.

7. Durante o prazo de dez anos a contar da data de colocação no mercado do produto com elementos digitais, os importadores devem manter um exemplar da declaração de conformidade UE à disposição das autoridades de fiscalização do mercado e assegurar que a documentação técnica possa ser facultada a essas autoridades, mediante pedido.

8. Mediante pedido fundamentado de uma autoridade de fiscalização do mercado, os importadores devem facultar-lhe toda a informação e documentação necessárias, em papel ou em suporte eletrónico, numa língua que possa ser facilmente compreendida por essa autoridade, para demonstrar a conformidade do produto com elementos digitais com os requisitos essenciais constantes do anexo I, secção 1, bem como a conformidade dos processos aplicados pelo fabricante com os requisitos essenciais constantes do anexo I, secção 2. Devem ainda cooperar com a referida autoridade, a pedido desta, no âmbito de quaisquer medidas tomadas para eliminar os riscos de cibersegurança decorrentes de um produto com elementos digitais que tenham colocado no mercado.

9. Quando tomar conhecimento de que o fabricante de um produto com elementos digitais cessou a sua atividade e, por conseguinte, não está em condições de cumprir as obrigações estabelecidas no presente regulamento, o importador do produto em causa deve informar desse facto as autoridades de fiscalização do mercado competentes, bem como os utilizadores dos produtos com elementos digitais colocados no mercado, por todos os meios disponíveis e tanto quanto possível.

Artigo 14.º

Obrigações dos distribuidores

1. Ao disponibilizarem um produto com elementos digitais no mercado, os distribuidores devem agir com a diligência devida em relação aos requisitos do presente regulamento.

2. Antes de disponibilizarem um produto com elementos digitais no mercado, os distribuidores devem certificar-se de que:

   (a) O produto com elementos digitais ostenta a marcação CE;

   (b) O fabricante e o importador cumpriram as obrigações estabelecidas no artigo 10.º, n.os 10 e 11, e no artigo 13.º, n.º 4, respetivamente.

3. Sempre que considere ou tenha motivos para crer que um produto com elementos digitais ou os processos aplicados pelo fabricante não estão em conformidade com os requisitos essenciais constantes do anexo I, o distribuidor não pode disponibilizar o produto em causa no mercado antes de se assegurar a conformidade do produto ou dos processos aplicados pelo fabricante. Além disso, se o produto com elementos digitais apresentar um risco de cibersegurança significativo, o distribuidor deve informar desse facto o fabricante e as autoridades de fiscalização do mercado.

4. Os distribuidores que saibam ou tenham motivos para crer que um produto com elementos digitais que colocaram no mercado, ou os processos aplicados pelo seu fabricante, não estão em conformidade com os requisitos essenciais constantes do anexo I devem garantir que são tomadas as medidas corretivas necessárias para assegurar a conformidade do produto em causa ou dos processos aplicados pelo seu fabricante, ou que retiram ou recolhem o produto, se for caso disso.

   Ao identificarem uma vulnerabilidade no produto com elementos digitais, os distribuidores devem informar o fabricante, sem demora injustificada, dessa vulnerabilidade. Além disso, se o produto com elementos digitais apresentar um risco de cibersegurança significativo, os distribuidores devem informar imediatamente desse facto as autoridades de fiscalização do mercado dos Estados-Membros em cujo mercado disponibilizaram o produto com elementos digitais, fornecendo-lhes as informações relevantes, sobretudo no que se refere à não conformidade e às medidas corretivas aplicadas.

5. Mediante pedido fundamentado de uma autoridade de fiscalização do mercado, os distribuidores devem facultar-lhe toda a informação e documentação necessárias, em papel ou em suporte eletrónico, numa língua que possa ser facilmente compreendida por essa autoridade, para demonstrar a conformidade do produto com elementos digitais e dos processos aplicados pelo respetivo fabricante com os requisitos essenciais constantes do anexo I. Devem ainda cooperar com a referida autoridade, a pedido desta, no âmbito de quaisquer medidas tomadas para eliminar os riscos de cibersegurança decorrentes de um produto com elementos digitais que tenham disponibilizado no mercado.

6. Quando tomar conhecimento de que o fabricante de um produto com elementos digitais cessou a sua atividade e, por conseguinte, não está em condições de cumprir as obrigações estabelecidas no presente regulamento, o distribuidor do produto em causa deve informar desse facto as autoridades de fiscalização do mercado competentes, bem como os utilizadores dos produtos com elementos digitais colocados no mercado, por todos os meios disponíveis e tanto quanto possível.

Artigo 15.º

Casos em que as obrigações dos fabricantes se aplicam aos importadores e distribuidores

Para efeitos do presente regulamento, os importadores ou os distribuidores são considerados fabricantes e ficam sujeitos às obrigações dos fabricantes estabelecidas no artigo 10.º e no

artigo 11.º, n.os 1, 2, 4 e 7, sempre que esses importadores ou distribuidores coloquem no mercado um produto com elementos digitais em seu nome ou ao abrigo de uma marca sua ou efetuem uma modificação substancial de um produto com elementos digitais já colocado no mercado.

Artigo 16.º

Outros casos em que se aplicam as obrigações dos fabricantes

Para efeitos do presente regulamento, a pessoa singular ou coletiva, distinta do fabricante, do importador ou do distribuidor, que proceda a uma modificação substancial do produto com elementos digitais é considerada um fabricante.

Esta pessoa fica sujeita às obrigações do fabricante estabelecidas no artigo 10.º e no artigo 11.º, n.os 1, 2, 4 e 7, relativamente à parte do produto afetada pela modificação substancial ou, se a modificação substancial afetar a cibersegurança do produto com elementos digitais no seu todo, relativamente a todo o produto.

Artigo 17.º

Identificação dos operadores económicos

1. Os operadores económicos devem, mediante pedido, facultar às autoridades de fiscalização do mercado as seguintes informações, sempre que disponíveis:

   (a) Nome e endereço de qualquer operador económico que lhes tenha fornecido um produto com elementos digitais;

   (b) Nome e endereço de qualquer operador económico a quem tenham fornecido um produto com elementos digitais.

2. Os operadores económicos devem estar em condições de apresentar as informações referidas no n.º 1 pelo prazo de dez anos após lhes ter sido fornecido o produto com elementos digitais e de dez anos após terem fornecido o produto com elementos digitais.

CAPÍTULO III

CONFORMIDADE DO PRODUTO COM ELEMENTOS DIGITAIS

Artigo 18.º

Presunção da conformidade

1. Presume-se que os produtos com elementos digitais e os processos aplicados pelo fabricante que estão em conformidade com as normas harmonizadas ou partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, estão conformes com os requisitos essenciais abrangidos pelas referidas normas ou partes destas, estabelecidos no anexo I.

2. Presume-se que os produtos com elementos digitais e os processos aplicados pelo fabricante que estão em conformidade com as especificações comuns a que se refere o artigo 19.º estão conformes com os requisitos essenciais constantes do anexo I, desde que tais especificações comuns abranjam esses requisitos.

3. Presume-se que os produtos com elementos digitais e os processos aplicados pelo fabricante para os quais tenha sido emitida uma declaração de conformidade UE ou um certificado ao abrigo de um sistema europeu de certificação da cibersegurança adotado nos termos do Regulamento (UE) 2019/881 e especificado nos termos do n.º 4 estão conformes com os requisitos essenciais estabelecidos no anexo I, desde que a declaração de conformidade UE ou o certificado de cibersegurança, ou partes destes, abranjam esses requisitos.

4. A Comissão fica habilitada a especificar, por meio de atos de execução, os sistemas europeus de certificação da cibersegurança adotados nos termos do Regulamento (UE) 2019/881 que podem ser utilizados para demonstrar a conformidade com os requisitos essenciais estabelecidos no anexo I, ou partes destes. Além disso, caso aplicável, a Comissão especifica se um certificado de cibersegurança emitido ao abrigo dos referidos sistemas elimina a obrigação que incumbe ao fabricante de realizar uma avaliação da conformidade por terceiros para os requisitos correspondentes, tal como estabelecido no artigo 24.º, n.º 2, alíneas a) e b), e n.º 3, alíneas a) e b). Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

Artigo 19.º

Especificações comuns

Se as normas harmonizadas referidas no artigo 18.º não existirem ou a Comissão considerar que as normas harmonizadas pertinentes são insuficientes para satisfazer os requisitos do presente regulamento ou para dar cumprimento ao pedido de normalização da Comissão, ou se houver atrasos indevidos no procedimento de normalização ou as organizações europeias de normalização não aceitarem o pedido de normas harmonizadas da Comissão, a Comissão fica habilitada a adotar, por meio de atos de execução, especificações comuns no que diz respeito aos requisitos essenciais estabelecidos no anexo I. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

Artigo 20.º

Declaração de conformidade UE

1. A declaração de conformidade UE é elaborada pelos fabricantes nos termos do artigo 10.º, n.º 7, e indica que o cumprimento dos requisitos essenciais aplicáveis constantes do anexo I foi demonstrado.

2. A declaração de conformidade UE respeita o modelo que consta do anexo IV e contém os elementos especificados nos procedimentos de avaliação da conformidade pertinentes que constam do anexo VI. A referida declaração deve ser permanentemente atualizada. Deve ser disponibilizada na língua ou línguas exigidas pelo Estado-Membro em cujo mercado o produto com elementos digitais é colocado ou disponibilizado.

3. Caso um produto com elementos digitais esteja abrangido por mais do que um ato da União que exija uma declaração de conformidade UE, deve ser elaborada uma declaração de conformidade UE única referente a todos esses atos da União. Essa declaração deve conter a identificação dos atos da União em causa, incluindo as respetivas referências de publicação.

4. Ao elaborar a declaração de conformidade UE, o fabricante assume a responsabilidade pela conformidade do produto.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 50.º para completar o presente regulamento acrescentando elementos ao conteúdo mínimo da declaração de conformidade UE constante do anexo IV, de forma a ter em conta a evolução tecnológica.

Artigo 21.º

Princípios gerais da marcação CE

A marcação CE, na aceção do artigo 3.º, ponto 32, está sujeita aos princípios gerais enunciados no artigo 30.º do Regulamento (CE) n.º 765/2008.

Artigo 22.º

Regras e condições para a aposição da marcação CE

1. A marcação CE deve ser aposta de modo visível, legível e indelével no produto com elementos digitais. Caso tal não seja possível ou não se justifique devido à natureza do produto com elementos digitais, a marcação CE deve ser aposta na embalagem e na declaração de conformidade UE referida no artigo 20.º que acompanha o produto com elementos digitais. No caso dos produtos com elementos digitais sob a forma de *software*, a marcação CE deve ser aposta na declaração de conformidade UE referida no artigo 20.º ou no sítio Web que acompanha o produto de *software*.

2. Tendo em conta a natureza do produto com elementos digitais, a altura da marcação CE aposta no produto com elementos digitais pode ser inferior a 5 mm, desde que continue a ser visível e legível.

3. A marcação CE deve ser aposta antes de o produto com elementos digitais ser colocado no mercado. Pode ser acompanhada de um pictograma ou de outra marca que indique um risco ou uma utilização especiais estabelecidos nos atos de execução referidos no n.º 6.

4. A marcação CE deve ser acompanhada do número de identificação do organismo notificado, sempre que este intervenha no procedimento de avaliação da conformidade baseada na garantia de qualidade total (baseado no módulo H) referido no artigo 24.º.

   O número de identificação do organismo notificado é aposto pelo próprio organismo ou, segundo as suas instruções, pelo fabricante ou pelo seu mandatário.

5. Os Estados-Membros devem basear-se nos mecanismos existentes para assegurarem a correta aplicação do regime que rege a marcação CE e devem tomar as medidas adequadas em caso de utilização indevida dessa marcação. Caso o produto com elementos digitais seja objeto de outra legislação da União que também preveja a aposição da marcação CE, a marcação deve indicar que o produto cumpre igualmente os requisitos dessa outra legislação.

6. A Comissão pode estabelecer, por meio de atos de execução, especificações técnicas para os pictogramas ou quaisquer outras marcas relacionadas com a segurança dos produtos com elementos digitais, bem como mecanismos para promover a sua utilização. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

Artigo 23.º

Documentação técnica

1. A documentação técnica contém todos os dados ou informações pertinentes sobre os meios utilizados pelo fabricante para assegurar que o produto com elementos digitais e os processos aplicados pelo fabricante cumprem os requisitos essenciais estabelecidos no anexo I. Deve conter, no mínimo, os elementos constantes do anexo V.

2. A documentação técnica deve ser elaborada antes de o produto com elementos digitais ser colocado no mercado e deve ser continuamente atualizada, se for caso disso, durante o tempo de vida esperado do produto ou por um período de cinco anos após a colocação do produto com elementos digitais no mercado, consoante o que for mais breve.

3. No caso dos produtos com elementos digitais referidos no artigo 8.º e no artigo 24.º, n.º 4, que também sejam abrangidos por outros atos da União, deve-se elaborar uma documentação técnica única que contenha as informações referidas no anexo V do presente regulamento e as informações exigidas por esses atos da União.

4. A documentação técnica e a correspondência relativas aos procedimentos de avaliação da conformidade devem ser redigidas numa língua oficial do Estado-Membro em que o organismo notificado está estabelecido ou numa língua aceite por esse organismo.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 50.º para completar o presente regulamento com os elementos a incluir na documentação técnica constante do anexo V, de modo a ter em conta a evolução tecnológica, bem como a evolução verificada no processo de execução do presente regulamento.

Artigo 24.º

Procedimentos de avaliação da conformidade dos produtos com elementos digitais

1. O fabricante deve realizar uma avaliação da conformidade do produto com elementos digitais e dos processos por ele aplicados de forma a determinar se são cumpridos os requisitos essenciais constantes do anexo I. Cabe ao fabricante ou ao seu mandatário demonstrar a conformidade com os requisitos essenciais recorrendo a um dos seguintes procedimentos:

   (a) O procedimento de controlo interno (com base no módulo A) constante do anexo VI; ou

   (b) O procedimento de exame UE de tipo (com base no módulo B) previsto no anexo VI, seguido da conformidade com o tipo UE baseada no controlo interno da produção (com base no módulo C) prevista no anexo VI; ou

   (c) A avaliação da conformidade baseada na garantia de qualidade total (com base no módulo H) prevista no anexo VI.

2. Sempre que, ao avaliar a conformidade do produto crítico com elementos digitais da classe I, conforme estabelecido no anexo III, e dos processos aplicados pelo seu fabricante com os requisitos essenciais constantes do anexo I, o fabricante ou o seu mandatário não tiver aplicado ou tiver aplicado apenas parcialmente normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança referidos no artigo 18.º, ou quando não existam tais normas

harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança, o produto com elementos digitais em causa e os processos aplicados pelo fabricante devem ser objeto, no que respeita a esses requisitos essenciais, de um dos seguintes procedimentos:

(a) O procedimento de exame UE de tipo (com base no módulo B) previsto no anexo VI, seguido da conformidade com o tipo UE baseada no controlo interno da produção (com base no módulo C) prevista no anexo VI; ou

(b) A avaliação da conformidade baseada na garantia de qualidade total (com base no módulo H) prevista no anexo VI.

3. Sempre que o produto for um produto crítico com elementos digitais da classe II, previsto no anexo III, o fabricante ou o seu mandatário deve demonstrar a conformidade com os requisitos essenciais constantes do anexo I recorrendo a um dos seguintes procedimentos:

(a) O procedimento de exame UE de tipo (com base no módulo B) previsto no anexo VI, seguido da conformidade com o tipo UE baseada no controlo interno da produção (com base no módulo C) prevista no anexo VI; ou

(b) A avaliação da conformidade baseada na garantia de qualidade total (com base no módulo H) prevista no anexo VI.

4. Os fabricantes de produtos com elementos digitais classificados como sistemas de RSE ao abrigo do Regulamento [Regulamento Espaço Europeu de Dados de Saúde] devem demonstrar a conformidade com os requisitos essenciais estabelecidos no anexo I do presente regulamento recorrendo ao procedimento de avaliação da conformidade pertinente exigido pelo Regulamento [capítulo III do Regulamento Espaço Europeu de Dados de Saúde].

5. Os organismos notificados devem ter em conta os interesses e necessidades específicos das pequenas e médias empresas (PME) aquando da definição das taxas aplicáveis aos procedimentos de avaliação da conformidade e proceder à redução das mesmas de forma proporcional aos referidos interesses e necessidades específicos.

CAPÍTULO IV

NOTIFICAÇÃO DOS ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Artigo 25.º

Notificação

Os Estados-Membros devem notificar a Comissão e os outros Estados-Membros dos organismos de avaliação da conformidade autorizados a realizar avaliações da conformidade ao abrigo do presente regulamento.

Artigo 26.º

Autoridades notificadoras

1. Os Estados-Membros devem designar uma autoridade notificadora responsável pela instauração e pela execução dos procedimentos necessários para a avaliação e a notificação dos organismos de avaliação da conformidade e para o controlo dos organismos notificados, incluindo no que respeita ao cumprimento do artigo 31.º.

2. Os Estados-Membros podem decidir que a avaliação e o controlo referidos no n.º 1 sejam efetuados por um organismo nacional de acreditação, na aceção e nos termos do Regulamento (CE) n.º 765/2008.

Artigo 27.º

Requisitos relativos às autoridades notificadoras

1. As autoridades notificadoras devem ser constituídas de modo a evitar conflitos de interesse com os organismos de avaliação da conformidade.

2. As autoridades notificadoras devem estar organizadas e funcionar de modo que garanta a objetividade e a imparcialidade das suas atividades.

3. As autoridades notificadoras devem estar organizadas de maneira que as decisões relativas à notificação do organismo de avaliação da conformidade sejam tomadas por pessoas competentes diferentes das que realizaram a avaliação.

4. As autoridades notificadoras não podem propor nem desempenhar nenhuma atividade que seja da competência dos organismos de avaliação da conformidade, nem prestar serviços de consultoria com caráter comercial ou em regime de concorrência.

5. As autoridades notificadoras devem garantir a confidencialidade das informações obtidas.

6. As autoridades notificadoras devem dispor de pessoal competente em número suficiente para o correto exercício das suas funções.

Artigo 28.º

Obrigação de informação das autoridades notificadoras

1. Os Estados-Membros devem informar a Comissão dos seus procedimentos de avaliação e notificação de organismos de avaliação da conformidade e de controlo dos organismos notificados, bem como de quaisquer alterações nessa matéria.

2. A Comissão deve disponibilizar essas informações ao público.

Artigo 29.º

Requisitos aplicáveis aos organismos notificados

1. Para efeitos de notificação, os organismos de avaliação da conformidade devem cumprir os requisitos previstos nos n.os 2 a 12.

2. Os organismos de avaliação da conformidade devem ser constituídos nos termos do direito nacional e ser dotados de personalidade jurídica.

3. Os organismos de avaliação da conformidade devem ser organismos terceiros independentes da organização ou do produto que avaliam.

Pode considerar-se como tal qualquer organismo que pertença a uma organização empresarial ou associação profissional representativa de empresas envolvidas em atividades de conceção, desenvolvimento, produção, fornecimento, montagem, utilização ou manutenção dos produtos com elementos digitais que avalia, desde que prove a respetiva independência e a inexistência de conflitos de interesse.

4. Os organismos de avaliação da conformidade, a sua direção de topo e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem ser o criador, o programador, o fabricante, o fornecedor, o instalador, o comprador, o proprietário, o utilizador ou o responsável pela manutenção dos produtos com elementos digitais que avaliam, nem o mandatário de qualquer uma dessas partes. Esta exigência não obsta à utilização de produtos avaliados que sejam necessários às atividades do organismo de avaliação da conformidade nem à utilização desses produtos para fins pessoais.

   Os organismos de avaliação da conformidade, a sua direção de topo e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem intervir diretamente na conceção, no desenvolvimento, na produção, na comercialização, na instalação, na utilização ou na manutenção desses produtos, nem representar as partes envolvidas nessas atividades. Não podem exercer nenhuma atividade suscetível de pôr em causa a independência da sua apreciação ou a sua integridade no desempenho das atividades de avaliação da conformidade para as quais são notificados. Esta disposição é aplicável nomeadamente aos serviços de consultoria.

   Os organismos de avaliação da conformidade devem certificar-se de que as atividades das suas filiais ou dos seus subcontratantes não afetam a confidencialidade, a objetividade e a imparcialidade das suas atividades de avaliação da conformidade.

5. Os organismos de avaliação da conformidade e o seu pessoal devem executar as suas atividades de avaliação da conformidade com a maior integridade profissional e a necessária competência técnica no domínio em causa e não podem estar sujeitos a nenhuma pressão ou incentivo, nomeadamente de ordem financeira, suscetível de influenciar a sua apreciação ou os resultados das suas atividades de avaliação da conformidade, em especial por parte de pessoas ou grupos de pessoas interessados nos resultados dessas atividades.

6. Os organismos de avaliação da conformidade devem ter capacidade para executar todas as tarefas de avaliação da conformidade referidas no anexo VI relativamente às quais tenham sido notificados, independentemente de as referidas tarefas serem executadas por si próprios ou em seu nome e sob a sua responsabilidade.

   Em todas as circunstâncias e para cada procedimento de avaliação da conformidade e para cada tipo ou categoria de produtos com elementos digitais para os quais tenham sido notificados, os organismos de avaliação da conformidade devem dispor de:

   (a) Pessoal com conhecimentos técnicos e experiência suficiente e adequada para executar as tarefas de avaliação da conformidade;

   (b) Descrições dos procedimentos de avaliação da conformidade que assegurem a transparência e a capacidade de reprodução desses procedimentos. Devem dispor de políticas e procedimentos apropriados para distinguir entre as tarefas executadas na qualidade de organismo notificado e qualquer outra atividade;

   (c) Procedimentos para o exercício das suas atividades que tenham em devida conta a dimensão, o setor e a estrutura das empresas, o grau de complexidade da tecnologia do produto em questão e a natureza do processo de produção em massa ou em série.

   Devem dispor dos meios necessários para desempenhar adequadamente as tarefas técnicas e administrativas ligadas à realização das atividades de avaliação da conformidade e devem ter acesso a todo o equipamento ou instalações necessários.

7. O pessoal responsável pela execução das atividades de avaliação da conformidade deve dispor de:

   (a) Uma sólida formação técnica e profissional, que abranja todas as atividades de avaliação da conformidade para as quais os organismos de avaliação da conformidade tenham sido notificados;

   (b) Um conhecimento satisfatório dos requisitos das avaliações que efetuam e a devida autoridade para as efetuar;

   (c) Conhecimento e compreensão adequados dos requisitos essenciais e das normas harmonizadas aplicáveis, bem como das disposições aplicáveis da legislação de harmonização da União e dos atos que lhes dão execução;

   (d) A aptidão para redigir os certificados, registos e relatórios comprovativos da realização das avaliações.

8. Deve ser garantida a imparcialidade dos organismos de avaliação da conformidade, da sua direção de topo e do pessoal encarregado da avaliação.

   A remuneração da direção de topo e do pessoal encarregado da avaliação dos organismos de avaliação da conformidade não pode depender do número de avaliações realizadas, nem do respetivo resultado.

9. Os organismos de avaliação da conformidade devem subscrever um seguro de responsabilidade civil, a não ser que essa responsabilidade seja coberta pelo Estado com base no direito nacional ou que o próprio Estado-Membro seja diretamente responsável pelas avaliações da conformidade.

10. O pessoal dos organismos de avaliação da conformidade está sujeito ao sigilo profissional no que se refere a todas as informações obtidas no desempenho das suas tarefas no âmbito do anexo VI ou de qualquer disposição de direito nacional que lhes dê aplicação, exceto em relação às autoridades de fiscalização do mercado do Estado-Membro em que exerce as suas atividades. Os direitos de propriedade devem ser protegidos. Os organismos de avaliação da conformidade devem dispor de procedimentos documentados que garantam o cumprimento do presente número.

11. Os organismos de avaliação da conformidade devem participar nas atividades de normalização relevantes e nas atividades do grupo de coordenação dos organismos notificados criado ao abrigo do artigo 40.º, ou assegurar que o pessoal encarregado de realizar a avaliação seja informado dessas atividades, e devem aplicar como orientações gerais as decisões e os documentos administrativos que resultem do trabalho desse grupo.

12. Os organismos de avaliação da conformidade devem funcionar de acordo com um conjunto de condições coerentes, justas e razoáveis, tendo particularmente em conta os interesses das PME no que respeita às taxas.

Artigo 30.º

Presunção da conformidade dos organismos notificados

Presume-se que os organismos de avaliação da conformidade que provem a sua conformidade com os critérios estabelecidos nas normas harmonizadas aplicáveis, ou em partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, cumprem os requisitos previstos no artigo 29.º, na medida em que as normas harmonizadas aplicáveis abranjam esses requisitos.

Artigo 31.º

Filiais e subcontratantes dos organismos notificados

1. Caso subcontrate tarefas específicas relacionadas com a avaliação da conformidade ou recorra a uma filial, o organismo notificado deve certificar-se de que o subcontratante ou a filial cumpre os requisitos previstos no artigo 29.º e informar a autoridade notificadora desse facto.

2. Os organismos notificados devem assumir plena responsabilidade pelas tarefas executadas por subcontratantes ou filiais, independentemente do local em que estes se encontram estabelecidos.

3. É indispensável o acordo do fabricante para que as atividades possam ser executadas por um subcontratante ou por uma filial.

4. Os organismos notificados devem manter à disposição da autoridade notificadora os documentos necessários respeitantes à avaliação das qualificações do subcontratante ou da filial e ao trabalho efetuado por estes nos termos do presente regulamento.

Artigo 32.º

Pedido de notificação

1. Os organismos de avaliação da conformidade devem apresentar um pedido notificação à autoridade notificadora do Estado-Membro onde se encontram estabelecidos.

2. O pedido deve ser acompanhado de uma descrição das atividades de avaliação da conformidade, do procedimento ou procedimentos de avaliação da conformidade e do produto ou produtos em relação aos quais os organismos se consideram competentes, bem como de um certificado de acreditação, se existir, emitido por um organismo nacional de acreditação, atestando que os organismos de avaliação da conformidade cumprem os requisitos estabelecidos no artigo 29.º.

3. Caso não possam apresentar o certificado de acreditação, os organismos de avaliação da conformidade devem fornecer à autoridade notificadora todas as provas documentais necessárias para a verificação, o reconhecimento e o controlo periódico da sua conformidade com os requisitos previstos no artigo 29.º.

Artigo 33.º

Procedimento de notificação

1. As autoridades notificadoras apenas podem notificar os organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 29.º.

2. A autoridade notificadora deve notificar a Comissão e os demais Estados-Membros por meio do sistema de informação NANDO, desenvolvido e gerido pela Comissão.

3. A notificação deve incluir dados completos das atividades de avaliação da conformidade, do(s) módulo(s) de avaliação da conformidade e do(s) produto(s) em causa, bem como a certificação de competência pertinente.

4. Se a notificação não se basear no certificado de acreditação referido no artigo 32.º, n.º 2, a autoridade notificadora deve facultar à Comissão e aos outros Estados-Membros provas documentais que atestem a competência técnica do organismo de avaliação da conformidade e as disposições introduzidas para assegurar que o

organismo será auditado periodicamente e continuará a cumprir os requisitos estabelecidos no artigo 29.º.

5. O organismo em causa só pode exercer as atividades de um organismo notificado se nem a Comissão nem os outros Estados-Membros tiverem levantado objeções nas duas semanas seguintes à notificação, caso seja utilizado um certificado de acreditação, e nos dois meses seguintes à notificação, caso não seja utilizada a acreditação.

   Apenas esse organismo pode ser considerado como organismo notificado para efeitos do presente regulamento.

6. A Comissão e os outros Estados-Membros devem ser notificados de todas as alterações relevantes subsequentemente introduzidas na notificação.

Artigo 34.º

Números de identificação e listas de organismos notificados

1. A Comissão deve atribuir um número de identificação a cada organismo notificado.

   O número atribuído é único, mesmo que o organismo esteja notificado ao abrigo de vários atos da União.

2. A Comissão deve publicar a lista de organismos notificados ao abrigo do presente regulamento, incluindo os números de identificação que lhes foram atribuídos e as atividades em relação às quais foram notificados.

   Cabe à Comissão garantir a atualização dessa lista.

Artigo 35.º

Alterações das notificações

1. Sempre que determinar ou for informada de que um organismo notificado deixou de cumprir os requisitos previstos no artigo 29.º ou de que não cumpre as suas obrigações, a autoridade notificadora deve restringir, suspender ou retirar a notificação, consoante o caso, em função da gravidade do incumprimento em causa. A autoridade notificadora deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto.

2. Em caso de restrição, suspensão ou retirada da notificação, ou caso o organismo notificado tenha cessado a sua atividade, o Estado-Membro notificador deve tomar as medidas necessárias para assegurar que os processos desse organismo sejam tratados por outro organismo notificado ou mantidos à disposição das autoridades notificadoras e das autoridades de fiscalização do mercado competentes, se estas o solicitarem.

Artigo 36.º

Contestação da competência dos organismos notificados

1. A Comissão deve investigar todos os casos em relação aos quais tenha dúvidas ou lhe sejam comunicadas dúvidas quanto à competência de determinado organismo notificado ou quanto ao cumprimento continuado por parte de um organismo notificado dos requisitos exigidos e das responsabilidades que lhe estão cometidas.

2. O Estado-Membro notificador deve facultar à Comissão, mediante pedido, todas as informações relacionadas com o fundamento da notificação ou a manutenção da competência do organismo em causa.

3. A Comissão deve assegurar que todas as informações sensíveis obtidas no decurso das suas investigações sejam tratadas de forma confidencial.

4. Sempre que determine que um organismo notificado não cumpre ou deixou de cumprir os requisitos que permitiram a sua notificação, a Comissão deve informar o Estado-Membro notificador desse facto e solicitar-lhe que tome as medidas corretivas necessárias, incluindo a retirada da notificação, se necessário.

Artigo 37.º

Obrigações operacionais dos organismos notificados

1. Os organismos notificados devem efetuar as avaliações da conformidade segundo os procedimentos de avaliação da conformidade previstos no artigo 24.º e no anexo VI.

2. As avaliações da conformidade devem ser efetuadas de modo proporcionado, evitando encargos desnecessários para os operadores económicos. Os organismos de avaliação da conformidade devem exercer as suas atividades tendo em devida conta a dimensão, o setor e a estrutura das empresas, o grau de complexidade da tecnologia do produto em questão e a natureza do processo de produção em massa ou em série.

3. Os organismos notificados devem, contudo, respeitar o grau de rigor e o nível de proteção exigidos para que o produto cumpra os requisitos do presente regulamento.

4. Se verificar que um fabricante não cumpriu os requisitos estabelecidos no anexo I, nas normas harmonizadas correspondentes ou nas especificações técnicas referidas no artigo 19.º, o organismo notificado deve exigir que o fabricante tome as medidas corretivas adequadas e não pode emitir um certificado de conformidade.

5. Se, durante o controlo da conformidade efetuado na sequência da emissão de um certificado, o organismo notificado verificar que o produto deixou de cumprir os requisitos do presente regulamento, deve exigir que o fabricante tome as medidas corretivas adequadas e deve suspender ou retirar o respetivo certificado, se necessário.

6. Se não forem tomadas medidas corretivas, ou se estas não tiverem o efeito pretendido, o organismo notificado deve restringir, suspender ou retirar os certificados, consoante o caso.

Artigo 38.º

Obrigação de informação dos organismos notificados

1. Os organismos notificados devem comunicar à autoridade notificadora as seguintes informações:

   (a) Qualquer recusa, restrição, suspensão ou retirada de certificados;

   (b) Quaisquer circunstâncias que afetem o âmbito e as condições de notificação;

   (c) Os pedidos de informação sobre as atividades de avaliação da conformidade efetuadas que tenham recebido das autoridades de fiscalização do mercado;

(d) Mediante pedido, as atividades de avaliação da conformidade que efetuaram no âmbito da respetiva notificação e todas as outras atividades efetuadas, nomeadamente atividades transfronteiriças e de subcontratação.

2. Os organismos notificados devem disponibilizar aos outros organismos notificados nos termos do presente regulamento que exerçam atividades de avaliação da conformidade semelhantes que abranjam os mesmos produtos as informações relevantes sobre questões relativas aos resultados negativos da avaliação da conformidade e, mediante pedido, aos resultados positivos.

Artigo 39.º

Intercâmbio de experiências

A Comissão deve organizar intercâmbios de experiências entre as autoridades nacionais dos Estados- Membros responsáveis pela política de notificação.

Artigo 40.º

Coordenação dos organismos notificados

1. A Comissão deve garantir a coordenação e a cooperação adequadas entre os organismos notificados, e que estas tenham lugar no âmbito de um grupo intersetorial de organismos notificados.

2. Os Estados-Membros devem assegurar que os organismos por si notificados participam, diretamente ou por meio de representantes designados, nos trabalhos desse grupo.

CAPÍTULO V

FISCALIZAÇÃO DO MERCADO E APLICAÇÃO DA LEGISLAÇÃO

Artigo 41.º

Fiscalização do mercado e controlo dos produtos com elementos digitais no mercado da União

1. O Regulamento (UE) 2019/1020 é aplicável aos produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento.

2. Cada Estado-Membro deve designar uma ou mais autoridades de fiscalização do mercado a fim de assegurar a efetiva execução do presente regulamento. Os Estados-Membros podem designar uma autoridade existente ou uma nova autoridade para atuar como autoridade de fiscalização do mercado para efeitos do presente regulamento.

3. Se for caso disso, as autoridades de fiscalização do mercado devem cooperar com as autoridades nacionais de certificação da cibersegurança designadas nos termos do artigo 58.º do Regulamento (UE) 2019/881 e proceder regularmente a um intercâmbio de informações. No que diz respeito à supervisão do cumprimento das obrigações de comunicação de informações nos termos do artigo 11.º do presente regulamento, as autoridades de fiscalização do mercado designadas devem cooperar com a ENISA.

4. Se for caso disso, as autoridades de fiscalização do mercado devem cooperar com outras autoridades de fiscalização do mercado designadas com base em legislação de harmonização da União relativa a outros produtos e proceder regularmente a um intercâmbio de informações.

5. As autoridades de fiscalização do mercado devem cooperar, conforme o caso, com as autoridades que supervisionam a legislação da União em matéria de proteção de dados. Tal cooperação inclui a informação dessas autoridades sobre qualquer constatação pertinente para o exercício das suas competências, nomeadamente aquando da emissão de orientações e prestação de aconselhamento nos termos do n.º 8 do presente artigo, se tal orientação e aconselhamento disserem respeito ao tratamento de dados pessoais.

   As autoridades que supervisionam a legislação da União em matéria de proteção de dados devem dispor de poderes para solicitar e aceder a qualquer documentação criada ou conservada ao abrigo do presente regulamento sempre que o acesso a essa documentação seja necessário para o desempenho das suas funções. As referidas autoridades devem informar as autoridades de fiscalização do mercado designadas do Estado-Membro em causa sobre tais pedidos.

6. Os Estados-Membros devem assegurar que as autoridades de fiscalização do mercado designadas disponham dos recursos financeiros e humanos adequados para exercerem as funções que lhes incumbem nos termos do presente regulamento.

7. A Comissão deve facilitar o intercâmbio de experiências entre as autoridades de fiscalização do mercado designadas.

8. As autoridades de fiscalização do mercado podem fornecer orientações e prestar aconselhamento aos operadores económicos sobre a execução do presente regulamento, com o apoio da Comissão.

9. As autoridades de fiscalização do mercado devem comunicar anualmente à Comissão os resultados das atividades de fiscalização do mercado pertinentes. As autoridades de fiscalização do mercado designadas devem comunicar, sem demora, à Comissão e às autoridades nacionais da concorrência competentes as informações identificadas no decurso de atividades de fiscalização do mercado que possam ter interesse para efeitos de aplicação do direito da concorrência da União.

10. No caso dos produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento classificados como sistemas de IA de risco elevado nos termos do artigo [artigo 6.º] do Regulamento [Regulamento Inteligência Artificial], as autoridades de fiscalização do mercado designadas para efeitos do Regulamento [Regulamento Inteligência Artificial] são as autoridades responsáveis pelas atividades de fiscalização do mercado exigidas por força do presente regulamento. As autoridades de fiscalização do mercado designadas nos termos do Regulamento [Regulamento Inteligência Artificial] devem cooperar, conforme o caso, com as autoridades de fiscalização do mercado designadas nos termos do presente regulamento e, no que diz respeito à supervisão do cumprimento das obrigações de comunicação de informações previstas no artigo 11.º, com a ENISA. As autoridades de fiscalização do mercado designadas nos termos do Regulamento [Regulamento Inteligência Artificial] devem, em especial, informar as autoridades de fiscalização do mercado designadas nos termos do presente regulamento de qualquer constatação pertinente para o desempenho das suas funções relacionada com a execução do presente regulamento.

11. É criado um grupo de cooperação administrativa (ADCO) específico para a aplicação uniforme do presente regulamento, nos termos do artigo 30.º, n.º 2, do Regulamento (UE) 2019/1020. O referido ADCO é composto por representantes das autoridades de fiscalização do mercado designadas e, se for caso disso, representantes dos serviços de ligação únicos.

Artigo 42.º

Acesso a dados e a documentação

Sempre que necessário para avaliar a conformidade dos produtos com elementos digitais e dos processos aplicados pelos seus fabricantes com os requisitos essenciais constantes do anexo I, e mediante pedido fundamentado, as autoridades de fiscalização do mercado devem ser autorizadas a aceder aos dados necessários para avaliar a conceção, o desenvolvimento, a produção e o tratamento de vulnerabilidades desses produtos, incluindo a documentação interna conexa do respetivo operador económico.

Artigo 43.º

Procedimento a nível nacional relativo a produtos com elementos digitais que apresentam um risco de cibersegurança significativo

1. Se tiver motivos suficientes para considerar que um produto com elementos digitais, incluindo o seu tratamento de vulnerabilidades, apresenta um risco de cibersegurança significativo, a autoridade de fiscalização do mercado de um Estado-Membro deve avaliar esse produto no que diz respeito ao cumprimento de todos os requisitos previstos no presente regulamento. Os operadores económicos envolvidos devem cooperar na medida do necessário com as autoridades de fiscalização do mercado.

   Sempre que, no decurso dessa avaliação, verifiquem que o produto com elementos digitais não cumpre os requisitos estabelecidos no presente regulamento, as autoridades de fiscalização do mercado devem exigir sem demora ao operador económico em causa que tome todas as medidas corretivas adequadas para assegurar a conformidade do produto com os requisitos mencionados, para o retirar do mercado ou para o recolher num prazo razoável que fixem e seja proporcional à natureza do risco.

   A autoridade de fiscalização do mercado deve informar desse facto o organismo notificado pertinente. O artigo 18.º do Regulamento (UE) 2019/1020 é aplicável às medidas corretivas adequadas.

2. Se considerar que a não conformidade não se limita ao respetivo território nacional, a autoridade de fiscalização do mercado deve comunicar à Comissão e aos outros Estados-Membros os resultados da avaliação e as medidas que exigiu que o operador tomasse.

3. Cabe ao fabricante assegurar que são tomadas todas as medidas corretivas adequadas relativamente a todos os produtos com elementos digitais em causa por si disponibilizados no mercado da União.

4. Caso o fabricante de um produto com elementos digitais não tome as medidas corretivas adequadas no prazo referido no n.º 1, segundo parágrafo, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a disponibilização do produto nos seus mercados nacionais, para o retirar do mercado ou para o recolher.

A referida autoridade deve informar sem demora a Comissão e os outros Estados-Membros da adoção de tais medidas.

5. A informação referida no n.º 4 deve conter todos os pormenores disponíveis, em especial os dados necessários à identificação dos produtos com elementos digitais não conformes, da origem do produto com elementos digitais, da natureza da alegada não conformidade e do risco conexo, da natureza e da duração das medidas nacionais tomadas, bem como os argumentos apresentados pelo operador em causa. As autoridades de fiscalização do mercado devem, nomeadamente, indicar se a não conformidade se deve a uma ou várias das seguintes razões:

   (a) Incumprimento da obrigação de o produto ou os processos aplicados pelo fabricante satisfazerem os requisitos essenciais constantes do anexo I;

   (b) Lacunas das normas harmonizadas, dos sistemas de certificação da cibersegurança ou das especificações comuns referidas no artigo 18.º.

6. As autoridades de fiscalização do mercado dos Estados-Membros, com exceção da autoridade de fiscalização do mercado do Estado-Membro que desencadeou o procedimento, devem informar sem demora a Comissão e os outros Estados-Membros das medidas tomadas e das informações adicionais de que disponham relativamente à não conformidade do produto em causa e, em caso de desacordo com a medida nacional notificada, das suas objeções.

7. Se, no prazo de três meses a contar da receção das informações referidas no n.º 4, nem os Estados-Membros nem a Comissão tiverem levantado objeções à medida provisória tomada por um Estado-Membro, considera-se que a mesma é justificada. Esta disposição aplica-se sem prejuízo dos direitos processuais do operador em causa previstos no artigo 18.º do Regulamento (UE) 2019/1020.

8. As autoridades de fiscalização do mercado de todos os Estados-Membros devem assegurar a aplicação imediata das medidas restritivas adequadas em relação ao produto em questão, como a sua retirada do respetivo mercado.

Artigo 44.º

Procedimento de salvaguarda da União

1. Se, nos três meses subsequentes à receção da notificação a que se refere o artigo 43.º, n.º 4, um Estado-Membro levantar objeções a uma medida tomada por outro Estado-Membro, ou a Comissão considerar que a medida é contrária à legislação da União, a Comissão deve iniciar sem demora consultas com o Estado-Membro e o operador ou operadores económicos em causa e avaliar a medida nacional. Em função dos resultados dessa avaliação, a Comissão decide se a medida nacional é ou não justificada no prazo de nove meses a contar da notificação referida no artigo 43.º, n.º 4, e notifica essa decisão ao Estado-Membro em causa.

2. Se a medida nacional for considerada justificada, todos os Estados-Membros devem tomar as medidas necessárias para garantir que o produto com elementos digitais não conforme seja retirado dos respetivos mercados, informando a Comissão desse facto. Se a medida nacional for considerada injustificada, o Estado-Membro em causa deve revogá-la.

3. Se a medida nacional for considerada justificada e a não conformidade do produto com elementos digitais for atribuída a lacunas das normas harmonizadas, a Comissão

deve aplicar o procedimento previsto no artigo 10.º do Regulamento (UE) n.º 1025/2012.

4. Se a medida nacional for considerada justificada e a não conformidade do produto com elementos digitais for atribuída a lacunas de um sistema europeu de certificação da cibersegurança referido no artigo 18.º, a Comissão deve ponderar a possibilidade de alterar ou revogar o ato de execução referido no artigo 18.º, n.º 4, que especifica a presunção de conformidade relativa a esse sistema de certificação.

5. Se a medida nacional for considerada justificada e a não conformidade do produto com elementos digitais for atribuída a lacunas das especificações comuns referidas no artigo 19.º, a Comissão deve ponderar a possibilidade de alterar ou revogar o ato de execução referido no artigo 19.º, que estabelece as referidas especificações comuns.

Artigo 45.º

Procedimento a nível da UE relativo a produtos com elementos digitais que apresentam um risco de cibersegurança significativo

1. Se tiver motivos suficientes para considerar, nomeadamente com base nas informações comunicadas pela ENISA, que um produto com elementos digitais que apresente um risco de cibersegurança significativo não está conforme com os requisitos estabelecidos no presente regulamento, a Comissão pode solicitar às autoridades de fiscalização do mercado competentes que efetuem uma avaliação da conformidade e sigam os procedimentos referidos no artigo 43.º.

2. Em circunstâncias excecionais que justifiquem uma intervenção imediata de modo a preservar o bom funcionamento do mercado interno e se a Comissão tiver motivos suficientes para considerar que o produto referido no n.º 1 continua a não estar conforme com os requisitos estabelecidos no presente regulamento e as autoridades de fiscalização do mercado competentes não tiverem tomado medidas eficazes, a Comissão pode solicitar à ENISA que proceda a uma avaliação da conformidade. A Comissão deve informar desse facto as autoridades de fiscalização do mercado competentes. Os operadores económicos envolvidos devem cooperar na medida do necessário com a ENISA.

3. Com base na avaliação da ENISA, a Comissão pode decidir que é necessária uma medida corretiva ou restritiva a nível da União. Para o efeito, deve consultar sem demora os Estados-Membros em causa e o operador ou operadores económicos em causa.

4. Com base na consulta referida no n.º 3, a Comissão pode adotar atos de execução de forma a decidir sobre medidas corretivas ou restritivas a nível da União, incluindo ordenando a retirada do mercado, ou a recolha, num prazo razoável, proporcional à natureza do risco. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

5. A Comissão deve comunicar imediatamente a decisão referida no n.º 4 ao operador ou operadores económicos em causa. Os Estados-Membros devem aplicar, sem demora, os atos referidos no n.º 4 e informar do facto a Comissão.

6. Os n.os 2 a 5 são aplicáveis durante o período de existência da situação excecional que justificou a intervenção da Comissão e enquanto o respetivo produto não estiver em conformidade com o presente regulamento.

Artigo 46.º

Produtos com elementos digitais conformes que apresentam um risco de cibersegurança significativo

1. Se, depois de efetuar a avaliação prevista no artigo 43.º, a autoridade de fiscalização do mercado de um Estado-Membro verificar que, não obstante o facto de estarem em conformidade com o presente regulamento, o produto com elementos digitais e os processos aplicados pelo fabricante apresentam um risco de cibersegurança significativo e, além disso, representam um risco para a saúde ou a segurança das pessoas, para o cumprimento de obrigações impostas pelo direito da União ou o direito nacional destinadas a proteger os direitos fundamentais, a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos serviços oferecidos através de um sistema de informação eletrónico por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)] ou para outros aspetos da proteção do interesse público, a referida autoridade deve exigir que o operador em causa tome todas as medidas adequadas para assegurar que o produto com elementos digitais e os processos aplicados pelo fabricante em causa já não apresentam esse risco quando o produto for colocado no mercado, para retirar o produto do mercado ou para o recolher num prazo razoável e proporcional à natureza do risco.

2. O fabricante ou outros operadores envolvidos devem assegurar que a medida corretiva seja tomada no tocante aos produtos com elementos digitais em causa que tenham disponibilizado no mercado da União no prazo fixado pela autoridade de fiscalização do mercado do Estado-Membro referida no n.º 1.

3. O Estado-Membro deve informar imediatamente a Comissão e os outros Estados-Membros sobre as medidas tomadas nos termos do n.º 1. Essas informações devem incluir todos os elementos disponíveis, nomeadamente os dados necessários para identificar o produto com elementos digitais em causa, a origem e a cadeia de abastecimento dos produtos com elementos digitais, a natureza do risco conexo e a natureza e duração das medidas nacionais tomadas.

4. A Comissão deve iniciar imediatamente consultas com os Estados-Membros e com o operador económico interessado e avaliar as medidas nacionais adotadas. Em função dos resultados dessa avaliação, a Comissão decide se a medida é ou não justificada e, se necessário, propõe medidas adequadas.

5. A Comissão designa os Estados-Membros como destinatários da decisão.

6. Se tiver motivos suficientes para considerar, nomeadamente com base nas informações comunicadas pela ENISA, que um produto com elementos digitais apresenta os riscos referidos no n.º 1, não obstante o facto de estar conforme com o presente regulamento, a Comissão pode solicitar à autoridade ou autoridades de fiscalização do mercado competentes que efetuem uma avaliação da conformidade e sigam os procedimentos referidos no artigo 43.º e no presente artigo, n.os 1, 2 e 3.

7. Em circunstâncias excecionais que justifiquem uma intervenção imediata de modo a preservar o bom funcionamento do mercado interno, se tiver motivos suficientes para considerar que o produto referido no n.º 6 continua a apresentar os riscos referidos no n.º 1 e as autoridades nacionais de fiscalização do mercado competentes não tiverem tomado medidas eficazes, a Comissão pode solicitar à ENISA que proceda a uma avaliação dos riscos que o produto em causa apresenta, devendo informar desse facto as autoridades de fiscalização do mercado competentes. Os operadores económicos envolvidos devem cooperar na medida do necessário com a ENISA.

8. Com base na avaliação da ENISA referida no n.º 7, a Comissão pode determinar que é necessária uma medida corretiva ou restritiva a nível da União. Para o efeito, deve consultar sem demora os Estados-Membros em causa e o operador ou operadores em causa.

9. Com base na consulta referida no n.º 8, a Comissão pode adotar atos de execução de forma a decidir sobre medidas corretivas ou restritivas a nível da União, incluindo ordenando a retirada do mercado, ou a recolha, num prazo razoável, proporcional à natureza do risco. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 51.º, n.º 2.

10. A Comissão deve comunicar imediatamente a decisão referida no n.º 9 ao operador ou operadores em causa. Os Estados-Membros devem aplicar sem demora esses atos e informar do facto a Comissão.

11. Os n.ºs 6 a 10 são aplicáveis durante o período de existência da situação excecional que justificou a intervenção da Comissão e enquanto o respetivo produto continuar a apresentar os riscos referidos no n.º 1.

Artigo 47.º

Não conformidade formal

1. Se a autoridade de fiscalização do mercado de um Estado-Membro constatar um dos factos a seguir enunciados, deve exigir ao fabricante em causa que ponha termo à não conformidade verificada:

   (a) A marcação de conformidade foi aposta em violação do disposto nos artigos 21.º e 22.º;

   (b) A marcação de conformidade não foi aposta;

   (c) A declaração de conformidade UE não foi elaborada;

   (d) A declaração de conformidade UE não foi elaborada corretamente;

   (e) O número de identificação do organismo notificado envolvido, se for caso disso, no procedimento de avaliação da conformidade não foi aposto;

   (f) A documentação técnica não está disponível ou não está completa.

2. Se a não conformidade referida no n.º 1 persistir, o Estado-Membro em causa deve tomar todas as medidas adequadas para restringir ou proibir a disponibilização no mercado do produto com elementos digitais ou para garantir que o mesmo seja recolhido ou retirado do mercado.

Artigo 48.º

Atividades conjuntas das autoridades de fiscalização do mercado

1. As autoridades de fiscalização do mercado podem acordar com outras autoridades competentes a realização de atividades conjuntas destinadas a garantir a cibersegurança e a proteção dos consumidores no que diz respeito a produtos com elementos digitais específicos colocados ou disponibilizados no mercado, em especial produtos que se constate frequentemente que apresentam riscos de cibersegurança.

2. A Comissão ou a ENISA podem propor a realização, pelas autoridades de fiscalização do mercado, de atividades conjuntas de verificação da conformidade com o presente regulamento, com base em indícios ou informações sobre uma potencial não conformidade, em vários Estados-Membros, de produtos abrangidos pelo âmbito de aplicação do presente regulamento com os requisitos estabelecidos neste último.

3. As autoridades de fiscalização do mercado e a Comissão, se for caso disso, devem assegurar que o acordo sobre a realização de atividades conjuntas não conduz a uma concorrência desleal entre os operadores económicos e não afeta negativamente a objetividade, a independência e a imparcialidade das partes do acordo.

4. As autoridades de fiscalização do mercado podem utilizar todas as informações resultantes de atividades realizadas no âmbito de uma investigação por si efetuada.

5. A autoridade de fiscalização do mercado em questão e a Comissão, se for caso disso, devem colocar à disposição do público o acordo sobre as atividades conjuntas, incluindo os nomes das partes envolvidas.

Artigo 49.º

Ações de fiscalização conjuntas («sweeps»)

1. As autoridades de fiscalização do mercado podem decidir realizar ações de controlo coordenadas simultâneas (ações de fiscalização conjuntas ou *sweeps*) de determinados produtos com elementos digitais ou categorias de tais produtos para verificar o cumprimento do presente regulamento ou detetar infrações ao mesmo.

2. Salvo acordo em contrário entre as autoridades de fiscalização do mercado envolvidas, as ações de fiscalização conjuntas são coordenadas pela Comissão. O coordenador da ação de fiscalização conjunta pode, se for caso disso, colocar à disposição do público os resultados agregados.

3. A ENISA pode identificar, no exercício das suas funções, nomeadamente com base nas notificações recebidas nos termos do artigo 11.º, n.os 1 e 2, as categorias de produtos para os quais podem ser organizadas ações de fiscalização conjuntas. A proposta de ação de fiscalização conjunta deve ser apresentada ao potencial coordenador referido no n.º 2 para apreciação das autoridades de fiscalização do mercado.

4. Ao efetuarem ações de fiscalização conjuntas, as autoridades de fiscalização do mercado que nelas participem podem exercer os poderes de investigação definidos nos artigos 41.º a 47.º e quaisquer outros poderes que lhes sejam conferidos pelo direito nacional.

5. As autoridades de fiscalização do mercado podem convidar funcionários da Comissão, e outros acompanhantes por esta autorizados, a participarem nas ações de fiscalização conjuntas.

CAPÍTULO VI

PODERES DELEGADOS E PROCEDIMENTO DE COMITÉ

Artigo 50.º

Exercício da delegação

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

2. O poder de adotar atos delegados referido no artigo 2.º, n.º 4, no artigo 6.º, n.os 2, 3 e 5, no artigo 20.º, n.º 5, e no artigo 23.º, n.º 5, é conferido à Comissão.

3. A delegação de poderes referida no artigo 2.º, n.º 4, no artigo 6.º, n.os 2, 3 e 5, no artigo 20.º, n.º 5, e no artigo 23.º, n.º 5, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

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

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

6. Os atos delegados adotados nos termos do artigo 2.º, n.º 4, do artigo 6.º, n.os 2, 3 e 5, do artigo 20.º, n.º 5, e do artigo 23.º, n.º 5, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 51.º

Procedimento de comité

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

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

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

CAPÍTULO VII

CONFIDENCIALIDADE E SANÇÕES

Artigo 52.º

Confidencialidade

1. Todas as partes envolvidas na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades de modo a proteger, em especial:

   (a) Os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte, exceto nos casos a que se refere o artigo 5.º da Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho[24];

   (b) A execução efetiva do presente regulamento, em especial no que diz respeito à realização de inspeções, investigações ou auditorias;

   (c) Interesses públicos e nacionais em matéria de segurança;

   (d) A integridade de processos penais ou administrativos.

2. Sem prejuízo do disposto no n.º 1, as informações trocadas confidencialmente entre as autoridades de fiscalização do mercado e entre estas e a Comissão não podem ser divulgadas sem acordo prévio da autoridade de fiscalização do mercado de origem.

3. O disposto nos n.os 1 e 2 não afeta os direitos e obrigações da Comissão, dos Estados-Membros e dos organismos notificados no que se refere ao intercâmbio de informações e à divulgação de avisos, nem o dever de informação que incumbe às pessoas em causa no âmbito do direito penal dos Estados-Membros.

4. A Comissão e os Estados-Membros podem, quando necessário, trocar informações sensíveis com autoridades competentes de países terceiros com as quais tenham celebrado acordos de confidencialidade bilaterais ou multilaterais que garantam um nível adequado de proteção.

Artigo 53.º

Sanções

1. Os Estados-Membros devem estabelecer as regras relativas às sanções aplicáveis às infrações ao presente regulamento cometidas pelos operadores económicos e tomar todas as medidas necessárias para assegurar a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros devem notificar sem demora a Comissão dessas regras e medidas e de qualquer alteração subsequente das mesmas.

3. A não conformidade com os requisitos essenciais de cibersegurança estabelecidos no anexo I e as obrigações previstas nos artigos 10.º e 11.º fica sujeita a coimas até

[24] Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de *know-how* e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais (JO L 157 de 15.6.2016, p. 1).

15 000 000 EUR ou, se o infrator for uma empresa, até 2,5 % do seu volume de negócios anual total a nível mundial no exercício anterior, consoante o que for mais elevado.

4. A não conformidade com qualquer outra obrigação prevista no presente regulamento fica sujeita a coimas até 10 000 000 EUR ou, se o infrator for uma empresa, até 2 % do seu volume de negócios anual total a nível mundial no exercício anterior, consoante o que for mais elevado.

5. O fornecimento de informações incorretas, incompletas ou enganadoras aos organismos notificados e às autoridades de fiscalização do mercado em resposta a um pedido fica sujeito a coimas até 5 000 000 EUR ou, se o infrator for uma empresa, até 1 % do seu volume de negócios anual total a nível mundial no exercício anterior, consoante o que for mais elevado.

6. A decisão relativa ao montante da coima a aplicar em cada caso deve ter em conta todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

   (a) A natureza, a gravidade e a duração da infração e das suas consequências;

   (b) Se outras autoridades de fiscalização do mercado já aplicaram coimas ao mesmo operador por uma infração semelhante;

   (c) A dimensão e quota de mercado do operador que cometeu a infração.

7. As autoridades de fiscalização do mercado que aplicam coimas devem partilhar essas informações com as autoridades de fiscalização do mercado de outros Estados-Membros através do sistema de informação e comunicação referido no artigo 34.º do Regulamento (UE) 2019/1020.

8. Cada Estado-Membro deve definir regras que permitam determinar se e em que medida podem ser aplicadas coimas às autoridades e organismos públicos estabelecidos no seu território.

9. Dependendo do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de maneira que as coimas sejam impostas por tribunais nacionais ou por outros organismos competentes, de acordo com as competências previstas a nível nacional nesses Estados- Membros. A aplicação dessas regras nesses Estados-Membros deve ter um efeito equivalente.

10. Atendendo às circunstâncias de cada caso, podem ser aplicadas coimas em cumulação com quaisquer outras medidas corretivas ou restritivas aplicadas pelas autoridades de fiscalização do mercado pela mesma infração.

CAPÍTULO VIII

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Artigo 54.º

Alteração do Regulamento (UE) 2019/1020

Ao anexo I do Regulamento (UE) 2019/1020 é aditado o seguinte ponto:

«71. [Regulamento XXX][Regulamento Ciber-Resiliência].».

Artigo 55.º

Disposições transitórias

1. Os certificados de exame UE de tipo e as decisões de aprovação relativos aos requisitos de cibersegurança de produtos com elementos digitais abrangidos por outra legislação de harmonização da União permanecem válidos até [42 meses após a data de entrada em vigor do presente regulamento], a menos que caduquem antes dessa data, ou salvo especificação em contrário noutra legislação da União, caso em que permanecem válidos nos termos dessa legislação da União.

2. Os produtos com elementos digitais que tenham sido colocados no mercado antes de [data de aplicação do presente regulamento referida no artigo 57.º] só ficam sujeitos aos requisitos do presente regulamento se, a partir dessa data, esses produtos forem objeto de modificações substanciais na sua conceção ou finalidade prevista.

3. Em derrogação do n.º 2, as obrigações estabelecidas no artigo 11.º são aplicáveis a todos os produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento que tenham sido colocados no mercado antes de [data de aplicação do presente regulamento referida no artigo 57.º].

Artigo 56.º

Avaliação e revisão

Até [36 meses após a data de aplicação do presente regulamento] e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão do presente regulamento. Os relatórios devem ser divulgados ao público.

Artigo 57.º

Entrada em vigor e aplicação

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

O presente regulamento é aplicável a partir de [24 meses após a data de entrada em vigor do presente regulamento]. Todavia, o artigo 11.º é aplicável a partir de [12 meses após a data de entrada em vigor do presente regulamento].

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangidos

1.3. A proposta/iniciativa refere-se a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(is)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultados e impacto esperados

1.4.4. Indicadores de desempenho

1.5. Justificação da proposta/iniciativa

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

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

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

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

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

1.6. Duração e impacto financeiro da proposta/iniciativa

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema(s) de gestão e de controlo

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

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

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

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

3.2. Impacto financeiro estimado nas dotações

3.2.1. Síntese do impacto estimado nas dotações operacionais

3.2.2. Estimativa das realizações financiadas com dotações operacionais

3.2.3. Síntese do impacto estimado nas dotações administrativas

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Proposta de regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais (Regulamento Ciber-Resiliência)

1.2. Domínio(s) de intervenção abrangidos

Redes de Comunicação, Conteúdos e Tecnologias

1.3. A proposta/iniciativa refere-se a:

× **uma nova ação**

☐ **uma nova ação na sequência de um projeto-piloto/ação preparatória**[37]

☐ **uma prorrogação de uma ação existente**

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

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(is)

A proposta tem dois objetivos principais, que visam assegurar o bom funcionamento do mercado interno: 1) **criar condições para o desenvolvimento de produtos com elementos digitais seguros,** garantindo que sejam colocados no mercado produtos de *hardware* e *software* com menos vulnerabilidades e que os fabricantes encarem a segurança com seriedade durante todo o ciclo de vida de um produto; e 2) **criar condições que permitam aos utilizadores ter em conta a cibersegurança aquando da seleção e da utilização de produtos com elementos digitais**.

1.4.2. Objetivo(s) específico(s)

Foram definidos **quatro objetivos específicos** para a proposta: i) assegurar que os fabricantes melhorem a segurança dos produtos com elementos digitais desde a fase de conceção e desenvolvimento e ao longo de todo o ciclo de vida; ii) assegurar um quadro de cibersegurança coerente, que facilite a conformidade por parte dos produtores de *hardware* e *software*; iii) aumentar a transparência das propriedades de segurança dos produtos com elementos digitais; e iv) permitir que as empresas e os consumidores utilizem produtos com elementos digitais de forma segura.

Resultados e impacto esperados

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

A proposta gerará vantagens significativas para as várias partes interessadas. Para as empresas, permitirá evitar a aplicação de regras de segurança divergentes aos produtos com elementos digitais e reduzir os custos de conformidade com a legislação conexa em matéria de cibersegurança. Reduzirá o número de ciberincidentes, os custos do tratamento de incidentes e os danos à reputação. Para a UE no seu conjunto, estima-se que a iniciativa possa conduzir a uma redução dos

[37] Tal como referido no artigo 58.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

custos decorrentes de incidentes que afetam as empresas de aproximadamente 180 a 290 mil milhões de EUR por ano[38]. Conduzirá a um aumento do volume de negócios em virtude do aumento da procura de produtos com elementos digitais. Melhorará a reputação global das empresas, levando a um aumento da procura também por parte de países terceiros. Para os utilizadores, a opção preferida reforçará a transparência das propriedades de segurança e facilitará a utilização de produtos com elementos digitais. Os consumidores e os cidadãos também beneficiarão de uma melhor proteção dos seus direitos fundamentais, como a privacidade e a proteção de dados.

Ao mesmo tempo, a proposta aumentará os custos de conformidade e de execução para as empresas, os organismos notificados e as autoridades públicas, incluindo as autoridades de acreditação e de fiscalização do mercado. Para os criadores de *software* e os fabricantes de *hardware*, aumentará os custos de conformidade diretos decorrentes de novos requisitos de segurança, da avaliação da conformidade, de obrigações em matéria de documentação e comunicação de informações, originando custos de conformidade agregados que ascendem a cerca de 29 mil milhões de EUR para um volume de negócios com valor de mercado estimado de 1,485 biliões de EUR[39]. Os utilizadores, incluindo os utilizadores profissionais, os consumidores e os cidadãos, podem ver-se confrontados com um aumento dos preços dos produtos com elementos digitais. No entanto, tal deve ser considerado no contexto dos benefícios significativos acima descritos.

1.4.3. Indicadores de desempenho

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

A fim de testar se os fabricantes melhoram a segurança dos seus produtos com elementos digitais desde a fase de conceção e desenvolvimento e em todo o ciclo de vida desses produtos, podem ser tidos em conta vários indicadores. Entre eles encontram-se o número de incidentes significativos na União causados por vulnerabilidades, a percentagem de fabricantes de *hardware* e criadores de *software* que adotam um ciclo de desenvolvimento sistematicamente seguro, uma análise qualitativa da segurança dos produtos com elementos digitais, uma avaliação quantitativa e qualitativa das bases de dados de vulnerabilidades, a frequência da disponibilização de atualizações corretivas de segurança pelos fabricantes ou o número médio de dias decorridos entre a descoberta de vulnerabilidades e a disponibilização de atualizações corretivas de segurança.

Um indicador para um quadro de cibersegurança coerente poderia ser a ausência de legislação nacional em matéria de cibersegurança direcionada e específica para cada produto.

Um indicador de transparência reforçada no que diz respeito às propriedades de segurança dos produtos com elementos digitais poderia ser a percentagem de produtos com elementos digitais que são expedidos com informações sobre as propriedades de segurança. Além disso, poder-se-ia utilizar a percentagem de produtos com elementos digitais que são expedidos com instruções de utilização

[38] Ver [documento de trabalho dos serviços da Comissão sobre o relatório da avaliação de impacto que acompanha o Regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais].

[39] Ver [documento de trabalho dos serviços da Comissão sobre o relatório da avaliação de impacto que acompanha o Regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais].

segura como indicador de que organizações e consumidores estão em posição de utilizar produtos com elementos digitais em segurança.

No que diz respeito ao acompanhamento do impacto do regulamento, serão tidos em consideração vários indicadores, que deverão ser avaliados pela Comissão, se for caso disso com o apoio da ENISA. Dependendo do objetivo operacional a alcançar, os indicadores de acompanhamento que permitirão avaliar o êxito dos requisitos horizontais de cibersegurança poderão ser, nomeadamente, os seguintes:

Para avaliar o nível de cibersegurança dos produtos com elementos digitais:

- Estatísticas e análises qualitativas sobre os incidentes que afetam produtos com elementos digitais e a sua gestão. Estas poderão ser recolhidas e avaliadas pela Comissão, com o apoio da ENISA.

- Registos de vulnerabilidades conhecidas e análise da forma como são tratadas. Essa análise poderá ser realizada pela ENISA, partindo da base de dados europeia de vulnerabilidades criada com base na [Diretiva XXX/XXXX (SRI 2)].

- Inquéritos junto dos fabricantes de *hardware* e *software* para acompanhar os progressos realizados.

Para avaliar o nível de informação sobre os elementos de segurança, o apoio prestado no domínio da segurança, o fim de vida e o dever de diligência: resultados dos inquéritos a realizar pela Comissão, com o apoio da ENISA, junto de utilizadores e empresas.

Para avaliar a execução, a Comissão procurará assegurar que as avaliações da conformidade são efetivamente realizadas. Para o efeito, emitir-se-á um pedido de normalização e acompanhar-se-á a sua execução. A Comissão verificará igualmente a capacidade dos organismos notificados e, se for caso disso, dos organismos de certificação.

No que diz respeito à aplicação, a Comissão verificará, através dos relatórios dos Estados-Membros, se as iniciativas nacionais não dizem respeito a aspetos abrangidos pelo regulamento.

1.5. Justificação da proposta/iniciativa

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

O regulamento deve ser plenamente aplicável 24 meses após a sua entrada em vigor. Contudo, antes dessa data devem já estar em funcionamento elementos da estrutura de governação. Em especial, os Estados-Membros devem ter designado autoridades existentes e/ou criado novas autoridades para a execução das funções definidas na legislação.

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

A natureza marcadamente transfronteiriça da cibersegurança e o aumento dos incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada. Dada a natureza global do mercado de produtos com elementos digitais, os Estados-Membros enfrentam, no respetivo território, os mesmos riscos para o mesmo produto com elementos digitais. A emergência de um mosaico de regras nacionais potencialmente divergentes poderá também prejudicar a criação de um mercado único aberto e competitivo para os produtos com elementos digitais. Torna-se, deste modo, necessária uma ação conjunta a nível da UE a fim de aumentar o nível de confiança entre os utilizadores e a atratividade dos produtos da UE com elementos digitais. Esta beneficiará igualmente o mercado interno, proporcionando segurança jurídica e criando condições de concorrência equitativas para os vendedores de produtos com elementos digitais.

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

O Regulamento Ciber-Resiliência é o primeiro ato legislativo do seu género, introduzindo requisitos de cibersegurança para a colocação no mercado de produtos com elementos digitais. Contudo, baseia-se na definição do novo quadro legislativo (NQL) e nos ensinamentos retirados do processo de aplicação da legislação de harmonização da União em vigor a uma série de produtos, nomeadamente no que diz respeito à preparação para a execução, incluindo aspetos como a elaboração de normas harmonizadas.

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

O Regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais define novos requisitos de cibersegurança para todos os produtos com elementos digitais colocados no mercado da UE, indo além dos requisitos previstos na legislação em vigor. Ao mesmo tempo, a proposta assenta na atual definição da legislação do NQL. Por conseguinte, basear-se-á nas estruturas e procedimentos existentes do NQL, tais como a cooperação dos organismos notificados e a fiscalização do mercado, os módulos de avaliação da conformidade e o desenvolvimento de normas harmonizadas. A nova proposta basear-se-á igualmente em algumas estruturas desenvolvidas de acordo com outra legislação em matéria de cibersegurança, como a Diretiva (UE) 2016/1148 (Diretiva SRI), a [Diretiva XXX/XXXX (SRI 2)], ou o Regulamento (UE) 2019/881 (Regulamento Cibersegurança).

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

A gestão dos domínios de ação atribuídos à ENISA enquadra-se no seu atual mandato e atribuições gerais. Estes domínios de ação podem exigir perfis específicos ou novas atribuições, mas estes não serão significativos, podendo ser absorvidos

pelos recursos existentes da ENISA e colmatados através da redistribuição ou da associação de várias atribuições. Por exemplo, um dos principais domínios de ação atribuídos à ENISA diz respeito à recolha e ao tratamento de notificações dos fabricantes sobre vulnerabilidades exploradas dos produtos. A [Diretiva XXX/XXXX (SRI 2)] já encarrega a ENISA de criar uma base de dados europeia de vulnerabilidades na qual se podem divulgar e registar, a título voluntário, as vulnerabilidades publicamente conhecidas, a fim de permitir que os utilizadores tomem as medidas de atenuação adequadas. Os recursos afetados para esse efeito também poderão ser utilizados para as novas atribuições, acima referidas, relativas às notificações de vulnerabilidades dos produtos. Tal poderá assegurar uma utilização eficaz dos recursos existentes e criará igualmente as sinergias necessárias entre essas atribuições, suscetíveis de melhorar as análises da ENISA sobre os riscos e as ameaças em matéria de cibersegurança.

1.6. Duração e impacto financeiro da proposta/iniciativa

☐ **duração limitada**

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

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

× **duração ilimitada**

– Aplicação com um período de arranque progressivo a partir de 2025,

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

1.7. Modalidade(s) de gestão prevista(s)[40]

☐ **Gestão direta** pela Comissão

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

– ☐ pelas agências de execução.

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

☐ **Gestão indireta** por delegação de tarefas de execução orçamental:

– ☐ em países terceiros ou nos organismos por estes designados;

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

– ☐ no BEI e no Fundo Europeu de Investimento;

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

– ☐ em organismos de direito público;

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

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

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

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

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

Observações

O presente regulamento confere à ENISA determinadas atribuições, em conformidade com o seu atual mandato, nomeadamente o artigo 3.º, n.º 2, do Regulamento (UE) 2019/881, que estabelece que a ENISA exerce as atribuições que lhe sejam conferidas por atos jurídicos da União que definam medidas para aproximar as disposições legislativas, regulamentares e administrativas dos Estados-Membros relacionadas com a cibersegurança. A ENISA é, em especial, incumbida de receber as notificações dos fabricantes relativas a vulnerabilidades ativamente exploradas existentes nos produtos com elementos digitais, bem como a incidentes que afetem a segurança desses produtos. A ENISA deve igualmente transmitir essas notificações às CSIRT competentes ou ao respetivo ponto de contacto único competente dos Estados-Membros designado nos termos do artigo [artigo X] da Diretiva [Diretiva XXX/XXXX (SRI 2)], bem como informar as autoridades de fiscalização do mercado. Com base nas informações que recolhe, a ENISA deve elaborar, de dois em dois anos, um relatório técnico sobre as tendências emergentes em matéria de riscos de cibersegurança de produtos com elementos digitais e apresentá-lo ao grupo de cooperação SRI. Além disso, tendo em conta os seus conhecimentos especializados, as informações recolhidas e as suas análises de ameaças, a ENISA pode apoiar o processo de execução do presente regulamento propondo atividades conjuntas a realizar pelas autoridades nacionais de fiscalização do mercado com base em indícios ou informações sobre a potencial não conformidade de produtos com elementos digitais com o presente regulamento em vários Estados-Membros ou identificar categorias de produtos para as quais podem ser organizadas ações de controlo coordenadas simultâneas. A Comissão pode solicitar à ENISA que realize avaliações de produtos específicos em circunstâncias excecionais respeitantes a produtos com elementos digitais que apresentem um risco de cibersegurança significativo e sempre que seja necessária uma intervenção imediata para preservar o bom funcionamento do mercado interno.

Prevê-se que todas estas tarefas representem cerca de 4,5 ETC, provenientes dos recursos existentes da ENISA, tirando já partido dos conhecimentos especializados e dos trabalhos preparatórios atualmente realizados pela ENISA, nomeadamente para apoiar a futura execução da [Diretiva XXX/XXXX (SRI 2)], que motivou a afetação de recursos suplementares à ENISA.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições.

Até 36 meses após a data de aplicação do presente regulamento e subsequentemente de quatro em quatro anos, a Comissão apresentará ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão. Os relatórios devem ser divulgados ao público.

2.2. Sistema(s) de gestão e de controlo

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

Este regulamento estabelece uma nova política em matéria de requisitos de cibersegurança harmonizados aplicáveis aos produtos com elementos digitais colocados no mercado interno ao longo de todo o seu ciclo de vida. O ato jurídico será seguido de pedidos de elaboração de normas dirigidos pela Comissão aos organismos europeus de normalização. Para desempenhar estas novas funções, é necessário dotar os serviços da Comissão dos recursos adequados. A execução do novo regulamento deverá exigir 7 ETC (dos quais um PND) de modo a abranger as seguintes tarefas:

- Elaboração do pedido de normalização e/ou de especificações comuns através de atos de execução, caso o processo de normalização não seja bem-sucedido;
- Elaboração de um ato delegado [no prazo de 12 meses a contar da data de entrada em vigor do regulamento] que especifique as definições dos produtos críticos com elementos digitais;
- Eventual elaboração de atos delegados para atualizar a lista de produtos críticos das classes I e II; especificar se é necessária uma limitação ou exclusão para produtos com elementos digitais abrangidos por outras regras da União que estabeleçam requisitos suscetíveis de alcançar o mesmo nível de proteção do presente regulamento; impor a certificação de determinados produtos altamente críticos com elementos digitais com base nos critérios estabelecidos no presente regulamento; especificar o conteúdo mínimo da declaração de conformidade UE e completar os elementos a incluir na documentação técnica;
- Eventual elaboração de atos de execução relativos ao formato ou aos elementos das obrigações de comunicação de informações, à lista de materiais do *software*, às especificações comuns ou à aposição da marcação CE;
- Eventual preparação de uma intervenção imediata para impor medidas corretivas ou restritivas em circunstâncias excecionais, a fim de preservar o bom funcionamento do mercado interno, incluindo a elaboração de um ato de execução;
- Organização e coordenação das notificações dos organismos notificados efetuadas pelos Estados-Membros e coordenação dos organismos notificados;
- Apoiar a coordenação das autoridades de fiscalização do mercado dos Estados-Membros.

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

A fim de assegurar a troca de informações e a boa cooperação entre os organismos notificados e as autoridades de fiscalização do mercado, a Comissão é responsável pela sua coordenação. Para as competências técnicas e de mercado, será criado um grupo de peritos.

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

2.3. Em relação às despesas de reunião, atendendo ao baixo valor por transação (por exemplo, reembolso das despesas de viagem de um representante para participar numa reunião), os procedimentos de controlo habituais afiguram-se suficientes. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas, por exemplo, a título da estratégia antifraude.

As atuais medidas de prevenção da fraude aplicáveis à Comissão cobrirão as dotações adicionais necessárias para efeitos do presente regulamento.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

- Atuais rubricas orçamentais

Esquema

- Novas rubricas orçamentais, cuja criação é solicitada

Não aplicável

3.2. Impacto financeiro estimado nas dotações

3.2.1. Síntese do impacto estimado nas dotações operacionais

– ☑ A proposta/iniciativa não acarreta a utilização de dotações operacionais.

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

Em milhões de EUR (três casas decimais)

Rubrica do quadro financeiro plurianual	Número	

DG: <…….>			Ano **N**[41]	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)			**TOTAL**
• Dotações operacionais										
Rubrica orçamental[42]	Autorizações	(1a)								
	Pagamentos	(2a)								
Rubrica orçamental	Autorizações	(1b)								
	Pagamentos	(2b)								
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos[43]										
Rubrica orçamental		(3)								
TOTAL das dotações para a DG <… >	Autorizações	= 1a+1b+3								
	Pagamentos	= 2a+2b +3								

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

42 De acordo com a nomenclatura orçamental oficial.

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

• TOTAL das dotações operacionais	Autorizações	(4)								
	Pagamentos	(5)								
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)								
TOTAL das dotações no âmbito da RUBRICA <….> do quadro financeiro plurianual	Autorizações	= 4 + 6								
	Pagamentos	= 5 + 6								

Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica operacional, repetir a secção acima:

• TOTAL das dotações operacionais (todas as rubricas operacionais)	Autorizações	(4)								
	Pagamentos	(5)								
TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos (todas as rubricas operacionais)		(6)								
TOTAL das dotações no âmbito das RUBRICAS 1 a 6 do quadro financeiro plurianual (quantia de referência)	Autorizações	= 4 + 6								
	Pagamentos	= 5 + 6								

Rubrica do quadro financeiro plurianual	**7**	«Despesas administrativas»

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

Em milhões de EUR (três casas decimais)

		Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
DG: CNECT						
• Recursos humanos		1,030	1,030	1,030	1,030	**4,120**
• Outras despesas administrativas		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTAL DG CNECT	Dotações	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTAL das dotações da RUBRICA 7 do quadro financeiro plurianual	(Total das autorizações = total dos pagamentos)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Em milhões de EUR (três casas decimais)

		Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
TOTAL das dotações no âmbito das RUBRICAS 1 a 7 do quadro financeiro plurianual	Autorizações	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Pagamentos	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Estimativa das realizações financiadas com dotações operacionais

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e as realizações ⇩			Ano **N**		Ano **N+1**		Ano **N+2**		Ano **N+3**		Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)						**TOTAL**	
			REALIZAÇÕES															
	Tipo[44]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º Total	Custo total
OBJETIVO ESPECÍFICO N.º 1[45]…																		
- Realização																		
- Realização																		
- Realização																		
Subtotal do objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2…																		
- Realização																		
Subtotal do objetivo específico n.º 2																		
TOTAIS																		

[44] As realizações dizem respeito aos produtos fornecidos e aos serviços prestados (por exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[45] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…»

3.2.3. Síntese do impacto estimado nas dotações administrativas

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

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

Em milhões de EUR (três casas decimais)

	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	
RUBRICA 7 do quadro financeiro plurianual					
Recursos humanos	1,030	1,030	1,030	1,030	**4,120**
Outras despesas administrativas	0,222	0,222	0,222	0,222	**0,888**
Subtotal RUBRICA 7 do quadro financeiro plurianual	1,252	1,252	1,252	1,252	**5,008**

Com exclusão da RUBRICA 7[46] **do quadro financeiro plurianual**					
Recursos humanos					
Outras despesas de natureza administrativa					
Subtotal com exclusão da RUBRICA 7 do quadro financeiro plurianual					

TOTAL	1,252	1,252	1,252	1,252	**5,008**

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

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

3.2.3.1. Necessidades estimadas de recursos humanos

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

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

As estimativas devem ser expressas em termos de equivalente a tempo completo

		Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**
20 01 02 01 (na sede e nos gabinetes de representação da Comissão)		6	6	6	6
20 01 02 03 (nas delegações)					
01 01 01 01 (investigação indireta)					
01 01 01 11 (investigação direta)					
Outras rubricas orçamentais (especificar)					
• Pessoal externo (em equivalente a tempo completo: ETC)[47]					
20 02 01 (AC, PND e TT da dotação global)		1	1	1	1
20 02 03 (AC, AL, PND, TT e JPD nas delegações)					
XX 01 xx **yy zz** [48]	- na sede				
	- nas delegações				
01 01 01 02 (AC, PND e TT - investigação indireta)					
01 01 01 12 (AC, PND e TT - investigação direta)					
Outras rubricas orçamentais (especificar)					
TOTAL		**7**	**7**	**7**	**7**

XX constitui o domínio de intervenção ou título em causa.

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

Descrição das tarefas a executar:

Funcionários e agentes temporários 6 ETC x 157 000 EUR/ano = 942 000 EUR	Tal como descrito no ponto 2.2.1.: – Elaboração do pedido de normalização e/ou de especificações comuns através de atos de execução, caso o processo de normalização não seja bem-sucedido; – Elaboração de um ato delegado [no prazo de 12 meses a contar da data de entrada em vigor do regulamento] que especifique as definições dos produtos críticos com elementos digitais; – Eventual elaboração de atos delegados para atualizar a lista de produtos críticos das classes I e II; especificar se é necessária uma limitação ou exclusão para produtos com elementos digitais abrangidos por outras regras da União que estabeleçam requisitos suscetíveis de alcançar o mesmo nível de proteção do presente regulamento; impor a certificação de determinados produtos altamente críticos com elementos digitais com base nos critérios estabelecidos no presente regulamento; especificar o conteúdo mínimo da declaração de conformidade UE e completar os elementos a incluir na

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

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

	documentação técnica; – Eventual elaboração de atos de execução relativos ao formato ou aos elementos das obrigações de comunicação de informações, à lista de materiais do *software*, às especificações comuns ou à aposição da marcação CE; – Eventual preparação de uma intervenção imediata para impor medidas corretivas ou restritivas em circunstâncias excecionais, a fim de preservar o bom funcionamento do mercado interno, incluindo a elaboração de um ato de execução; – Organização e coordenação das notificações dos organismos notificados efetuadas pelos Estados-Membros e coordenação dos organismos notificados; – Apoiar a coordenação das autoridades de fiscalização do mercado dos Estados-Membros.
Pessoal externo 1 PND x 88 000 EUR/ano	Tal como descrito no ponto 2.2.1.: – Elaboração do pedido de normalização e/ou de especificações comuns através de atos de execução, caso o processo de normalização não seja bem-sucedido; – Elaboração de um ato delegado [no prazo de 12 meses a contar da data de entrada em vigor do regulamento] que especifique as definições dos produtos críticos com elementos digitais; – Eventual elaboração de atos delegados para atualizar a lista de produtos críticos das classes I e II; especificar se é necessária uma limitação ou exclusão para produtos com elementos digitais abrangidos por outras regras da União que estabeleçam requisitos suscetíveis de alcançar o mesmo nível de proteção do presente regulamento; impor a certificação de determinados produtos altamente críticos com elementos digitais com base nos critérios estabelecidos no presente regulamento; especificar o conteúdo mínimo da declaração de conformidade UE e completar os elementos a incluir na documentação técnica; – Eventual elaboração de atos de execução relativos ao formato ou aos elementos das obrigações de comunicação de informações, à lista de materiais do *software*, às especificações comuns ou à aposição da marcação CE; – Eventual preparação de uma intervenção imediata para impor medidas corretivas ou restritivas em circunstâncias excecionais, a fim de preservar o bom funcionamento do mercado interno, incluindo a elaboração de um ato de execução; – Organização e coordenação das notificações dos organismos notificados efetuadas pelos Estados-Membros e coordenação dos organismos notificados; – Apoio à coordenação das autoridades de fiscalização do mercado dos Estados-Membros.

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

A proposta/iniciativa:

– x pode ser integralmente financiada por meio da reafetação de fundos no quadro da rubrica pertinente do quadro financeiro plurianual (QFP).

Não é necessária reprogramação.

– ☐ requer o recurso à margem não afetada na rubrica em causa do QFP e/ou o recurso a instrumentos especiais tais como definidos no Regulamento QFP.

-

– ☐ requer uma revisão do QFP.

-

3.2.5. Participação de terceiros no financiamento

A proposta/iniciativa:

– x não prevê o cofinanciamento por terceiros

– ☐ prevê o seguinte cofinanciamento por terceiros, a seguir estimado:

Dotações em milhões de EUR (três casas decimais)

	Ano **N**[49]	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)			Total
Especificar o organismo de cofinanciamento								
TOTAL das dotações cofinanciadas								

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

3.3. Impacto estimado nas receitas

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

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

  – ☐ nos recursos próprios

  – ☐ noutras receitas

  – indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o atual exercício	Impacto da proposta/iniciativa[50]						
		Ano **N**	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)		
Artigo …….								

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

Outras observações (p. ex., método/fórmula de cálculo do impacto nas receitas ou quaisquer outras informações).

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