Jornal Oficial
da União Europeia

PT
Série L

2024/2847

20.11.2024

REGULAMENTO (UE) 2024/2847 DO PARLAMENTO EUROPEU E DO CONSELHO

de 23 de outubro de 2024

relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência)

(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]),

Após consulta ao Comité das Regiões,

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

Considerando o seguinte:

(1) A cibersegurança é um dos desafios fundamentais para a União. O número e a variedade de dispositivos conectados aumentarão exponencialmente nos próximos anos. Os ciberataques constituem um assunto de interesse público, pois têm um impacto crítico não só na economia da União, mas também na democracia, bem como na saúde e segurança dos consumidores. É, portanto, necessário reforçar a abordagem da União à cibersegurança, incidir sobre a ciber-resiliência a nível da União e melhorar o funcionamento do mercado interno estabelecendo um regime 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, por exemplo melhorando a transparência no tocante ao período de apoio para produtos com elementos digitais disponibilizados no mercado.

(3) O direito pertinente da União 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, o direito da União em vigor em matéria de cibersegurança, nomeadamente o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([3]) e a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([4]), não abrange diretamente os requisitos obrigatórios de segurança dos produtos com elementos digitais.

([1]) JO C 100 de 16.3.2023, p. 101.
([2]) Posição do Parlamento Europeu de 12 de março de 2024 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 10 de outubro de 2024.
([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]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

(4) Embora o direito da União em vigor se aplique a determinados produtos com elementos digitais, não existe um regime 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 e organizações no cumprimento de uma série de requisitos e obrigações para tipos semelhantes de produtos. A cibersegurança desses produtos tem uma dimensão transfronteiriça particularmente forte, uma vez que os produtos com elementos digitais fabricados num Estado-Membro ou num país terceiro são muitas vezes utilizados por organizações e consumidores em todo o mercado interno, o que torna necessário regulamentar este domínio a nível da União de molde a garantir um regime regulamentar harmonizado e segurança jurídica para os utilizadores, organizações e empresas, designadamente as micro, pequenas e médias empresas, tal como definido no anexo da Recomendação 2003/361/CE da Comissão ([5]). O panorama regulamentar da União deverá ser harmonizado através da introdução de requisitos horizontais de cibersegurança para os produtos com elementos digitais. Além disso, deverão ser asseguradas em toda a União a segurança jurídica para os operadores económicos e utilizadores, uma melhor harmonização do mercado interno e proporcionalidade para as micro, pequenas e médias empresas, criando condições mais viáveis para os operadores económicos que pretendam entrar no mercado da União.

(5) No que concerne às microempresas e às pequenas e médias empresas, aquando da determinação da categoria em que uma empresa se insere, as disposições do anexo da Recomendação 2003/361/CE deverão ser aplicadas na sua totalidade. Por conseguinte, ao calcular o número de efetivos e os limiares financeiros que estabelecem as categorias de empresas, deverão igualmente ser aplicadas as disposições do artigo 6.º do anexo da Recomendação 2003/361/CE relativas à determinação dos dados de uma empresa tendo em conta tipos específicos de empresas, tais como empresas parceiras ou associadas.

(6) A Comissão deverá fornecer orientações para ajudar os operadores económicos, em especial as micro, pequenas e médias empresas, na aplicação do presente regulamento. Tais orientações deverão abranger, nomeadamente, o âmbito de aplicação do presente regulamento, em particular o tratamento remoto de dados e as suas implicações para os criadores de *software* livre e de código-fonte aberto, a aplicação dos critérios utilizados para determinar os períodos de apoio aos produtos com elementos digitais, a interação entre o presente regulamento e outro direito da União e o conceito de «modificação substancial».

(7) A nível da União, vários documentos programáticos e políticos, como a Comunicação conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 16 de dezembro de 2020, intitulada «Estratégia de Cibersegurança da UE para a Década Digital», as Conclusões do Conselho de 2 de dezembro de 2020 sobre a cibersegurança dos dispositivos conectados e de 23 de maio de 2022 sobre o desenvolvimento da postura da União Europeia no ciberespaço e a Resolução do Parlamento Europeu, de 10 de junho de 2021, sobre a Estratégia de Cibersegurança da UE para a década digital ([6]), apelaram à criação de requisitos específicos da União em matéria de cibersegurança para produtos digitais ou conectados, sendo que vários países terceiros introduziram medidas para resolver esta questão por sua própria iniciativa. No relatório final da Conferência sobre o Futuro da Europa, os cidadãos apelaram ao reforço do papel da União na luta contra as ameaças à cibersegurança. É importante estabelecer um regime regulamentar ambicioso, para que a União possa desempenhar um papel de liderança a nível internacional no domínio da cibersegurança.

(8) 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 esses produtos, que sejam orientados para objetivos, tecnologicamente neutros e horizontalmente aplicáveis.

(9) 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 como sendo menos críticos podem resultar no comprometimento inicial de um dispositivo ou rede, permitindo que agentes mal-intencionados obtenham acesso privilegiado a um sistema ou circulem lateralmente entre sistemas. Os fabricantes deverão, por conseguinte, assegurar que todos os produtos com elementos digitais sejam concebidos e desenvolvidos em conformidade com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento. Essa obrigação refere-se aos 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 ciberameaças 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 deverão também garantir a cibersegurança dos produtos com elementos digitais que só estão indiretamente conectados a outros dispositivos ou redes.

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

([6]) JO C 67 de 8.2.2022, p. 81.

(10) A especificação de requisitos de cibersegurança para a colocação de produtos com elementos digitais no mercado destina-se a reforçar a cibersegurança desses produtos, tanto para os consumidores como para as empresas. Esses requisitos garantirão também que a cibersegurança seja tida em conta em todas as cadeias de abastecimento, tornando os produtos finais com elementos digitais e os respetivos componentes mais seguros. Estes incluem igualmente requisitos para a colocação no mercado de produtos de consumo com elementos digitais destinados a consumidores vulneráveis, tais como brinquedos e sistemas de vigilância de bebés. Os produtos de consumo com elementos digitais classificados no presente regulamento como produtos importantes com elementos digitais apresentam um risco de cibersegurança mais elevado ao desempenharem uma função que comporta um risco significativo de produzir efeitos adversos, pela sua intensidade e capacidade de prejudicar a saúde, a segurança ou a proteção dos utilizadores desses produtos, e deverão ser sujeitos a um procedimento de avaliação da conformidade mais rigoroso. Incluem-se nesta descrição, entre outros, os produtos domésticos inteligentes com funcionalidades de segurança, nomeadamente fechaduras de porta inteligentes, sistemas de vigilância de bebés e sistemas de alarme inteligentes, brinquedos conectados e tecnologias de saúde pessoais vestíveis. Além disso, os procedimentos de avaliação da conformidade mais rigorosos a que devem ser submetidos outros produtos com elementos digitais classificados no presente regulamento como produtos importantes ou críticos com elementos digitais contribuirão para evitar potenciais consequências negativas que a exploração de vulnerabilidades pudesse acarretar para os consumidores.

(11) O objetivo do presente regulamento é assegurar um elevado nível de cibersegurança dos produtos com elementos digitais e das respetivas soluções de tratamento integrado remoto de dados. Tais soluções de tratamento remoto de dados deverão ser definidas como qualquer tratamento de dados à distância para o qual o *software* tenha sido concebido e desenvolvido pelo fabricante dos produtos com elementos digitais em causa ou em seu nome e cuja inexistência impediria o produto com elementos digitais de desempenhar uma das suas funções. Essa abordagem garante a proteção adequada de tais produtos na sua totalidade pelos respetivos fabricantes, independentemente de os dados serem tratados ou armazenados localmente no dispositivo do utilizador ou à distância pelo fabricante. Ao mesmo tempo, o tratamento ou o armazenamento à distância só são abrangidos pelo âmbito de aplicação do presente regulamento na medida em que seja necessário para que um produto com elementos digitais desempenhe as suas funções. Esse tratamento ou armazenamento à distância inclui os casos em que uma aplicação móvel exija o acesso a uma interface de programação de aplicações ou a uma base de dados fornecida por meio de um serviço desenvolvido pelo fabricante. Nesses casos, o serviço é abrangido pelo âmbito de aplicação do presente regulamento enquanto solução de tratamento remoto de dados. Os requisitos relativos às soluções de tratamento remoto de dados abrangidas pelo âmbito de aplicação do presente regulamento não implicam, por conseguinte, medidas técnicas, operacionais ou organizativas destinadas a gerir os riscos para a segurança da rede e dos sistemas de informação de um fabricante no seu conjunto.

(12) As soluções em nuvem apenas constituem soluções de tratamento remoto de dados na aceção do presente regulamento se corresponderem à definição nele estabelecida. Por exemplo, as funcionalidades possibilitadas pela computação em nuvem, fornecidas por um fabricante de dispositivos domésticos inteligentes, que permitem aos utilizadores controlar o dispositivo à distância, devem ser abrangidas pelo âmbito de aplicação do presente regulamento. Por outro lado, os sítios Web que não suportam a funcionalidade de um produto com elementos digitais ou serviços de computação em nuvem que não sejam concebidos e desenvolvidos sob a responsabilidade do fabricante de um produto com elementos digitais são excluídos do âmbito de aplicação do presente regulamento. A Diretiva (UE) 2022/2555 é aplicável aos serviços de computação em nuvem e aos modelos de serviços de computação em nuvem, tais como o *software* como serviço (SaaS, do inglês «Software as a Service»), a plataforma como serviço (PaaS, do inglês «Platform as a Service») ou as infraestruturas como serviço (IaaS, do inglês «Infrastructure as a Service»). As entidades que prestem serviços de computação em nuvem na União e que sejam consideradas médias empresas nos termos do artigo 2.º do anexo da Recomendação 2003/361/CE, ou que excedem os limiares para as médias empresas previstos no n.º 1 do mesmo artigo, são abrangidas pelo âmbito de aplicação da referida diretiva.

(13) Em consonância com os objetivos do presente regulamento de eliminar os obstáculos à livre circulação de produtos com elementos digitais, 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. Por conseguinte, no concernente às questões harmonizadas pelo presente regulamento, os Estados-Membros não podem impor requisitos de cibersegurança adicionais para a disponibilização no mercado de produtos com elementos digitais. No entanto, qualquer entidade, pública ou privada, pode estabelecer requisitos adicionais aos definidos no presente regulamento para a aquisição ou utilização de produtos com elementos digitais para os seus fins específicos, podendo, como tal, optar por utilizar produtos com elementos digitais que cumpram requisitos de cibersegurança mais rigorosos ou mais específicos do que os aplicáveis à disponibilização no mercado ao abrigo do presente regulamento. Sem prejuízo das Diretivas 2014/24/UE ([7]) e 2014/25/UE ([8]) do Parlamento Europeu e do Conselho, aquando da aquisição de produtos com elementos digitais, que devem cumprir os requisitos essenciais de cibersegurança estabelecidos no presente regulamento, incluindo os relativos ao tratamento de

([7]) Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

([8]) Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos celebrados pelas entidades que operam nos setores da água, da energia, dos transportes e dos serviços postais e que revoga a Diretiva 2004/17/CE (JO L 94 de 28.3.2014, p. 243).

vulnerabilidades, os Estados-Membros deverão assegurar que esses requisitos são tidos em conta no processo de aquisição e que é também tida em conta a capacidade dos fabricantes para aplicarem eficazmente medidas de cibersegurança e gerirem ciberameaças. Além disso, a Diretiva (UE) 2022/2555 estabelece medidas de gestão dos riscos de cibersegurança para as entidades essenciais e importantes a que se refere o artigo 3.º da mesma diretiva que podem implicar medidas de segurança da cadeia de abastecimento que exijam a utilização, por parte dessas entidades, de produtos com elementos digitais que cumpram requisitos de cibersegurança mais rigorosos do que os definidos no presente regulamento. Em conformidade com a Diretiva (UE) 2022/2555 e de acordo com o seu princípio de harmonização mínima, os Estados-Membros podem, assim, impor requisitos adicionais de cibersegurança para a utilização de produtos de tecnologias da informação e comunicação (TIC) por entidades essenciais ou importantes nos termos da referida diretiva, visando assegurar um nível mais elevado de cibersegurança, desde que esses requisitos sejam coerentes com as obrigações dos Estados-Membros estabelecidas no direito da União. As matérias não abrangidas pelo presente regulamento podem incluir fatores não técnicos relativos a produtos com elementos digitais e aos respetivos fabricantes. Por conseguinte, os Estados-Membros podem estabelecer medidas nacionais, incluindo restrições aos produtos com elementos digitais ou aos fornecedores desses produtos, que tenham em conta fatores não técnicos. As medidas nacionais relativas a esses fatores devem respeitar o direito da União.

(14) O presente regulamento não deverá prejudicar a responsabilidade dos Estados-Membros de salvaguardar a segurança nacional, em conformidade com o direito da União. Os Estados-Membros deverão poder submeter a medidas adicionais os produtos com elementos digitais adquiridos ou utilizados para fins de segurança ou de defesa nacionais, desde que essas medidas sejam coerentes com as obrigações dos Estados-Membros estabelecidas no direito da União.

(15) O presente regulamento aplica-se aos operadores económicos apenas em relação a produtos com elementos digitais disponibilizados no mercado e, portanto, fornecidos para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial. O fornecimento no âmbito de uma atividade comercial pode caracterizar-se não só pela cobrança de um preço por um produto com elementos digitais, mas também pela cobrança de um preço pelos serviços de apoio técnico se não for apenas no intuito de recuperar os custos reais, por uma intenção de monetizar, por exemplo, pela disponibilização de uma plataforma de *software* através da qual o fabricante monetize outros serviços, pela exigência do tratamento de dados pessoais como condição para a utilização por razões que não sejam exclusivamente destinadas a melhorar a segurança, a compatibilidade ou a interoperabilidade do *software*, ou pela aceitação de donativos que ultrapassem os custos associados com a conceção, o desenvolvimento e a produção de um produto com elementos digitais. A aceitação de donativos sem intenção de fazer lucro não deverá ser considerada uma atividade comercial.

(16) Os produtos com elementos digitais fornecidos no contexto da prestação de um serviço pelo qual é cobrada uma taxa unicamente para recuperar os custos reais diretamente relacionados com o funcionamento desse serviço, como pode ocorrer no caso de determinados produtos com elementos digitais fornecidos por entidades da administração pública, não deverão ser considerados, meramente por esses motivos, uma atividade comercial para efeitos do presente regulamento. Ademais, os produtos com elementos digitais desenvolvidos ou modificados por uma entidade da administração pública exclusivamente para uso próprio não deverão ser considerados como sendo disponibilizados no mercado na aceção do presente regulamento.

(17) O *software* e os dados que sejam partilhados abertamente e que possam, eles próprios ou uma versão alterada dos mesmos, ser livremente acedidos, utilizados, alterados e redistribuídos pelos utilizadores podem contribuir para a investigação e para a inovação no mercado. Para promover o desenvolvimento e a utilização de *software* livre e de código fonte aberto, sobretudo pelas micro, pequenas e médias empresas, incluindo as empresas em fase de arranque, pelos particulares, pelas organizações sem fins lucrativos e por organizações de investigação académica, a aplicação do presente regulamento a produtos com elementos digitais que sejam considerados *software* livre e de código-fonte aberto fornecido para distribuição ou utilização no âmbito de uma atividade comercial deverá ter em conta a natureza dos diferentes modelos de desenvolvimento de *software* distribuído e desenvolvido no quadro de licenças de *software* livre e de código-fonte aberto.

(18) O *software* livre e de código-fonte aberto é entendido como um *software* cujo código-fonte é partilhado abertamente e cuja licença prevê todos os direitos para que seja livremente acessível, utilizável, modificável e redistribuível. O *software* livre e de código-fonte aberto é desenvolvido, mantido e distribuído abertamente, inclusive através de plataformas em linha. No tocante aos operadores económicos abrangidos pelo âmbito de aplicação do presente regulamento, apenas o *software* livre e de código-fonte aberto disponibilizado no mercado, e, por conseguinte, fornecido para distribuição ou utilização no âmbito de uma atividade comercial, deverá ser abrangido pelo âmbito de aplicação do presente regulamento. As meras circunstâncias em que o produto com elementos digitais foi desenvolvido ou a forma como o desenvolvimento foi financiado não deverão, assim, ser tidas em conta para determinar a natureza comercial ou não comercial da atividade em causa. Mais especificamente, para efeitos do presente regulamento e em relação aos operadores económicos abrangidos pelo âmbito de aplicação do mesmo, a fim de assegurar uma distinção clara entre as fases de desenvolvimento e de fornecimento, a produção de produtos

com elementos digitais que se qualifiquem como *software* livre e de código-fonte aberto e que não sejam monetizados pelos seus fabricantes não deverá ser considerada como sendo uma atividade comercial. Além disso, o fornecimento de produtos com elementos digitais que se qualifiquem como componentes de *software* livre e de código-fonte aberto destinados à integração por outros fabricantes nos seus próprios produtos com elementos digitais só deverá ser considerado como disponibilização no mercado se o componente for monetizado pelo seu fabricante original. Por exemplo, o simples facto de um produto de *software* de código-fonte aberto com elementos digitais receber apoio financeiro dos fabricantes ou de os fabricantes contribuírem para o desenvolvimento desse produto não deverá, por si só, determinar que a atividade é de natureza comercial. Além disso, a mera existência de atualizações regulares não deverá, por si só, levar à conclusão de que um produto com elementos digitais é fornecido no âmbito de uma atividade comercial. Por último, para efeitos do presente regulamento, o desenvolvimento de produtos com elementos digitais que se qualifiquem como *software* livre e de código-fonte aberto por organizações sem fins lucrativos não deverá ser considerado uma atividade comercial, desde que a organização esteja criada de forma a garantir que todas as receitas após os custos sejam utilizadas para alcançar objetivos sem fins lucrativos. O presente regulamento não se aplica às pessoas singulares ou coletivas que contribuam com código-fonte para produtos com elementos digitais considerados *software* livre e de código-fonte aberto que não estejam sob a sua responsabilidade.

(19) Tendo em conta a importância para a cibersegurança de muitos produtos com elementos digitais considerados *software* livre e de código-fonte aberto que são lançados, mas não disponibilizados no mercado na aceção do presente regulamento, as pessoas coletivas que prestam apoio sistemático ao desenvolvimento desses produtos destinados a atividades comerciais e que desempenham um papel importante na garantia da viabilidade desses produtos (administradores de *software* de código-fonte aberto) deverão ser sujeitas a um regime regulamentar pouco restritivo e adaptado. Entre os administradores de *software* de código-fonte aberto contam-se determinadas fundações e entidades que desenvolvem e lançam *software* livre e de código-fonte aberto num contexto empresarial, nomeadamente entidades sem fins lucrativos. O regime regulamentar deverá ter em conta a natureza específica e a compatibilidade de tais entidades com o tipo de obrigações impostas. Deverá abranger apenas os produtos com elementos digitais considerados *software* livre e de código-fonte aberto que, em última análise, se destinam a atividades comerciais, como a integração em serviços comerciais ou em produtos monetizados com elementos digitais. Para efeitos desse regime regulamentar, uma intenção de integração em produtos monetizados com elementos digitais abarca os casos em que os fabricantes que integram um componente nos seus próprios produtos com elementos digitais contribuem regularmente para o desenvolvimento desse componente ou prestam assistência financeira regular para assegurar a continuidade de um produto de *software*. A prestação de apoio sistemático ao desenvolvimento de um produto com elementos digitais inclui, entre outros, o alojamento e a gestão de plataformas de colaboração para o desenvolvimento de *software*, o alojamento de código-fonte ou *software*, a administração ou gestão de produtos com elementos digitais que sejam considerados *software* livre e de código-fonte aberto, bem como a orientação do desenvolvimento desses produtos. Uma vez que o regime regulamentar simplificado e adaptado não sujeita quem atue na qualidade de administradores de *software* de código-fonte aberto às mesmas obrigações a que está sujeito quem atue como fabricante ao abrigo do presente regulamento, não lhes deverá ser autorizada a aposição da marcação CE nos produtos com elementos digitais cujo desenvolvimento apoiam.

(20) O simples ato de alojar produto com elementos digitais em repositórios abertos, designadamente através de gestores de pacotes ou em plataformas de colaboração, não constitui, por si só, a disponibilização no mercado de um produto com elementos digitais. Os prestadores destes serviços só deverão ser considerados distribuidores se disponibilizarem tal *software* no mercado e, portanto, o fornecerem para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial.

(21) Com vista a apoiar e facilitar o cumprimento da diligência devida dos fabricantes que integrem nos seus produtos com elementos digitais componentes de *software* livre e de código-fonte aberto que não estejam sujeitos aos requisitos essenciais de cibersegurança previstos no presente regulamento, a Comissão deverá poder estabelecer programas voluntários de certificação de segurança, quer através de um ato delegado que complete o presente regulamento, quer solicitando um sistema europeu de certificação da cibersegurança nos termos do artigo 48.º do Regulamento (UE) 2019/881 que tenha em conta as especificidades dos modelos de desenvolvimento de *software* livre e de código-fonte aberto. Os programas de certificação de segurança deverão ser concebidos de modo que não só as pessoas singulares ou coletivas que desenvolvam ou contribuam para o desenvolvimento de um produto com elementos digitais considerados *software* livre e de código-fonte aberto possam iniciar ou financiar uma certificação de segurança, mas também terceiros, como os fabricantes que integram esses produtos nos seus próprios produtos com elementos digitais, utilizadores ou administrações públicas nacionais e da União.

(22) À luz dos objetivos de cibersegurança pública do presente regulamento e a fim de melhorar o conhecimento da situação dos Estados-Membros no tocante à dependência da União em relação a componentes de *software* e, em especial, a componentes de *software* potencialmente livres e de código-fonte aberto, um grupo de cooperação administrativa (ADCO) específico criado pelo presente regulamento deverá poder decidir realizar conjuntamente uma avaliação da dependência da União. As autoridades de fiscalização do mercado deverão poder solicitar aos fabricantes de categorias de produtos com elementos digitais estabelecidas pelo ADCO que apresentem as listas de materiais do *software* (LMS) que estabeleceram nos termos do presente regulamento. A fim de proteger a confidencialidade das LMS, as autoridades de fiscalização do mercado deverão apresentar ao ADCO informações pertinentes sobre dependências, de forma anonimizada e agregada.

(23) A eficácia da aplicação do presente regulamento dependerá igualmente da disponibilidade de competências adequadas em matéria de cibersegurança. Ao nível da União, diversos documentos programáticos e políticos, incluindo a Comunicação da Comissão, de 18 de abril de 2023, intitulada «Colmatar o défice de talentos no domínio da cibersegurança para reforçar a competitividade, o crescimento e a resiliência da UE» e as Conclusões do Conselho de 22 de maio de 2023 sobre a política de ciberdefesa da UE, reconheceram o défice de competências existente na União em matéria de cibersegurança e a necessidade de dar resposta a esses desafios com caráter prioritário, tanto no setor público como no privado. Visando garantir uma aplicação eficaz do presente regulamento, os Estados-Membros deverão assegurar a disponibilidade de recursos adequados para dotar de pessoal apropriado as autoridades de fiscalização do mercado e os organismos de avaliação da conformidade, para que possam desempenhar as suas funções, estabelecidas no presente regulamento. Essas medidas deverão reforçar a mobilidade da mão de obra no domínio da cibersegurança e os respetivos percursos profissionais. Deverão ainda contribuir para tornar a mão de obra no domínio da cibersegurança mais resiliente e inclusiva, também no tocante ao género. Os Estados-Membros deverão, por conseguinte, tomar medidas para assegurar que essas tarefas sejam desempenhadas por profissionais com formação adequada e as competências necessárias em matéria de cibersegurança. Do mesmo modo, os fabricantes deverão assegurar que o respetivo pessoal possua as competências necessárias para cumprir as obrigações que lhe incumbem por força do presente regulamento. Os Estados-Membros e a Comissão, em consonância com as suas prerrogativas e competências e com as atribuições específicas que lhes são conferidas pelo presente regulamento, deverão tomar medidas para apoiar os fabricantes, em especial as micro, pequenas e médias empresas, incluindo as empresas em fase de arranque, também em domínios como o desenvolvimento de competências, para efeitos do cumprimento das suas obrigações estabelecidas no presente regulamento. Adicionalmente, uma vez que a Diretiva (UE) 2022/2555 exige que os Estados-Membros adotem políticas que promovam e desenvolvam formação em cibersegurança e competências em matéria de cibersegurança no âmbito das suas estratégias nacionais de cibersegurança, os Estados-Membros também podem ponderar, ao adotar essas estratégias, se devem dar resposta às necessidades de competências de cibersegurança decorrentes do presente regulamento, incluindo as relacionadas com a requalificação e a melhoria de competências.

(24) Uma internet segura é indispensável para o funcionamento das infraestruturas críticas e para a sociedade no seu conjunto. A Diretiva (UE) 2022/2555 visa garantir um elevado nível de cibersegurança aos serviços prestados por entidades essenciais e importantes a que se refere o artigo 3.º da mesma diretiva, incluindo os fornecedores de infraestruturas digitais que apoiam as funções essenciais da Internet aberta e asseguram o acesso à Internet e a prestação de 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 (UE) 2022/2555, 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.

(25) O Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho ([9]) estabelece regras relativas aos dispositivos médicos e o Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho ([10]) estabelece regras relativas aos dispositivos médicos para diagnóstico in vitro. Os referidos 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. Esses 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 previstos no anexo I desses regulamentos no que diz respeito à cibersegurança. Os produtos com elementos digitais a que se aplique qualquer um desses regulamentos não deverão, por conseguinte, ser abrangidos pelo presente regulamento.

(26) Não são abrangidos pelo âmbito de aplicação do presente regulamento os produtos com elementos digitais desenvolvidos ou modificados exclusivamente para fins de defesa ou de segurança nacional que tenham sido especificamente concebidos para o tratamento de informações classificadas. Os Estados-Membros são incentivados a assegurar um nível de proteção para esses produtos igual ou superior ao dos que se inserem no âmbito de aplicação do presente regulamento.

([9]) 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).

([10]) 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).

(27) O Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho ([11]) estabelece requisitos de homologação de veículos e dos seus sistemas e componentes, 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 de cibersegurança 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, nomeadamente o 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 ([12]), e prevendo procedimentos específicos de avaliação da conformidade. No domínio da aviação, o Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho ([13]) tem como objetivo principal estabelecer e manter um nível elevado e uniforme de segurança da aviação civil na União. Cria um regime para os requisitos essenciais de aeronavegabilidade dos produtos, peças e equipamentos aeronáuticos, incluindo o *software*, que abrange as obrigações de proteção contra ameaças à segurança da informação. O processo de certificação previsto no Regulamento (UE) 2018/1139 assegura o nível de garantia visado no presente regulamento. 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 deverão estar, por conseguinte, sujeitos aos requisitos essenciais de cibersegurança e aos procedimentos de avaliação da conformidade estabelecidos no presente regulamento.

(28) 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 de cibersegurança previstos 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 de cibersegurança estabelecidos no presente regulamento, pode ser limitada ou excluída se essa limitação ou exclusão for coerente com o regime regulamentar global aplicável a esses produtos e se as regras setoriais permitirem alcançar pelo menos o mesmo nível de proteção que o previsto no presente regulamento. A Comissão deverá ficar habilitada a adotar atos delegados para completar o presente regulamento, identificando os referidos produtos e regras. O presente regulamento prevê disposições específicas que clarificam a sua relação com o direito da União em vigor que implique a aplicação dessa limitação ou exclusão.

(29) A fim de garantir que os produtos com elementos digitais disponibilizados no mercado possam ser reparados eficazmente e que a sua durabilidade seja alargada, deverá ser prevista uma isenção para as peças sobresselentes. Essa isenção deverá cobrir as peças sobresselentes destinadas a reparar produtos antigos, disponibilizados antes da data de aplicação do presente regulamento, bem como as peças sobresselentes que já tenham sido sujeitas a um procedimento de avaliação da conformidade nos termos do presente regulamento.

(30) O Regulamento Delegado (UE) 2022/30 da Comissão ([14]) especifica que alguns requisitos essenciais estabelecidos no artigo 3.º, n.º 3, alíneas d), e) e f), da Diretiva 2014/53/UE do Parlamento Europeu e do Conselho ([15]), referentes a danos na rede e utilização inadequada dos recursos da rede, dados pessoais e privacidade e fraude, se aplicam a determinados equipamentos de rádio. A Decisão de Execução C(2022)5637 da Comissão, de 5 de agosto de 2022, relativa a um pedido de normalização ao Comité Europeu de Normalização e ao Comité Europeu de Normalização Eletrotécnica estabelece requisitos para o desenvolvimento de normas específicas que definam melhor a forma como esses requisitos essenciais deverão ser tratados. Os requisitos essenciais de cibersegurança previstos 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. Adicionalmente, os requisitos essenciais de cibersegurança previstos no presente regulamento

([11]) 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).

([12]) JO L 82 de 9.3.2021, p. 30.

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

([14]) Regulamento Delegado (UE) 2022/30 da Comissão, de 29 de outubro de 2021, que complementa a Diretiva 2014/53/UE do Parlamento Europeu e do Conselho no que diz respeito à aplicação dos requisitos essenciais referidos no artigo 3.º, n.º 3, alíneas d), e) e f), dessa diretiva (JO L 7 de 12.1.2022, p. 6).

([15]) Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62).

harmonizam-se com os objetivos dos requisitos para a elaboração de normas específicas incluídos nesse pedido de normalização. Por conseguinte, quando 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 deverão ter em conta o trabalho de normalização realizado no contexto da Decisão de Execução C(2022)5637 na elaboração e no desenvolvimento de normas harmonizadas para facilitar a aplicação do presente regulamento. Durante o período de transição para aplicação do presente regulamento, a Comissão deverá fornecer orientações aos fabricantes abrangidos pelo presente regulamento que estejam igualmente sujeitos ao Regulamento Delegado (UE) 2022/30, para facilitar a demonstração da conformidade com ambos os regulamentos.

(31) A Diretiva (UE) 2024/2853 do Parlamento Europeu e do Conselho ([16]) 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 deverão ser estabelecidas no presente regulamento.

(32) O presente regulamento não deverá prejudicar o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([17]), incluindo as disposições relacionadas com o 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, criado pelo Regulamento (UE) 2016/679, e as autoridades nacionais de controlo da proteção de dados. Deverão também ser criadas sinergias entre o presente regulamento 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 deverão cooperar com as autoridades responsáveis pela supervisão da aplicação da legislação da União em matéria de proteção de dados. Estas últimas deverão igualmente ter acesso às informações pertinentes para o desempenho das suas funções.

(33) Na medida em que os seus produtos sejam abrangidos pelo âmbito de aplicação do presente regulamento, os fornecedores de carteiras europeias de identidade digital a que se refere o artigo 5.º-A, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([18]), deverão cumprir os requisitos essenciais horizontais de cibersegurança previstos no presente regulamento e os requisitos de segurança específicos previstos no artigo 5.º-A do Regulamento (UE) n.º 910/2014. A fim de facilitar o cumprimento, os fornecedores de carteiras digitais deverão poder demonstrar a conformidade das carteiras europeias de identidade digital com os requisitos estabelecidos no presente regulamento e no Regulamento (UE) n.º 910/2014, respetivamente, 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, por meio de atos delegados, uma presunção de conformidade com o presente regulamento, contanto que o certificado, ou partes do mesmo, abranja esses requisitos.

(34) Ao integrarem componentes provenientes de terceiros em produtos com elementos digitais durante a fase de conceção e desenvolvimento, os fabricantes deverão, no intuito de assegurar que os produtos sejam concebidos, desenvolvidos e produzidos em conformidade com os requisitos essenciais de cibersegurança previstos no presente regulamento, exercer a diligência devida no que diz respeito a esses componentes, incluindo componentes de *software*

([16]) Diretiva (UE) 2024/2853 do Parlamento Europeu do Conselho, de 23 de outubro de 2024, relativa à responsabilidade decorrente dos produtos defeituosos e que revoga a Diretiva 85/374/CEE do Conselho (JO L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

livre e de código-fonte aberto que não tenham sido disponibilizados no mercado. O nível adequado de diligência devida depende da natureza e do nível de risco de cibersegurança associado a um determinado componente e deverá, para o efeito, ter em conta uma ou mais das seguintes ações: verificar, consoante o caso, se o fabricante de um componente demonstrou a conformidade com o disposto no presente regulamento, nomeadamente confirmando se o componente já ostenta a marcação CE; verificar se um componente recebe atualizações de segurança regulares, por exemplo, através da confirmação do seu historial de atualizações de segurança; verificar se um componente está isento de vulnerabilidades registadas na base de dados europeia de vulnerabilidades, criada nos termos do artigo 12.º, n.º 2, da Diretiva (UE) 2022/2555, ou noutras bases de dados de vulnerabilidades acessíveis ao público; ou realizar testes de segurança adicionais. As obrigações em matéria de tratamento de vulnerabilidades estabelecidas no presente regulamento, que os fabricantes têm de cumprir quando colocam um produto com elementos digitais no mercado e durante o período de apoio, aplicam-se aos produtos com elementos digitais na sua totalidade, incluindo todos os componentes integrados. Se, no exercício da diligência devida, o fabricante do produto com elementos digitais identificar uma vulnerabilidade num componente, incluindo num componente livre e de código-fonte aberto, deverá informar a pessoa ou entidade responsável pelo fabrico ou pela manutenção do componente, analisar e corrigir a vulnerabilidade e, se for caso disso, disponibilizar a essa pessoa ou entidade a solução de segurança aplicada.

(35) Imediatamente após o período de transição para a aplicação do presente regulamento, o fabricante de um produto com elementos digitais que integre um ou vários componentes provenientes de terceiros que também estejam sujeitos ao presente regulamento pode não conseguir verificar, no âmbito da sua obrigação de diligência devida, se os fabricantes desses componentes demonstraram a conformidade com o disposto no presente regulamento, verificando, por exemplo, se os componentes já ostentam a marcação CE. Pode ser o caso se os componentes tiverem sido integrados antes de o presente regulamento se tornar aplicável aos fabricantes desses componentes. Nesse caso, o fabricante que integre esses componentes deverá exercer a diligência devida por outros meios.

(36) Para que possam circular livremente dentro do mercado interno, os produtos com elementos digitais deverão apresentar a marcação CE para indicar de modo visível, legível e indelével 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. Ademais, em feiras comerciais, exposições e demonstrações ou eventos semelhantes, os Estados-Membros não deverão impedir a apresentação ou utilização de um produto com elementos digitais que não cumpra o disposto no presente regulamento, designadamente dos seus protótipos, contanto que seja apresentado com um sinal visível que indique nitidamente que o produto não cumpre o disposto no presente regulamento e que não deve ser disponibilizado no mercado até que o cumpra.

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

(38) 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, deverão ser estabelecidos requisitos essenciais de cibersegurança para esses produtos. Esses requisitos essenciais de cibersegurança, incluindo os requisitos de gestão do tratamento de vulnerabilidades, aplicam-se a cada produto individual com elementos digitais quando for colocado no mercado, independentemente de o produto com elementos digitais ser fabricado como uma unidade individual ou em série. Por exemplo, para um tipo de produto, cada produto individual com elementos digitais deverá ter recebido todas as atualizações corretivas de segurança ou outras atualizações disponíveis para resolver os problemas de segurança pertinentes aquando da sua colocação no mercado. Se os produtos com elementos digitais forem subsequentemente modificados, através de meios físicos ou digitais, de uma forma que não esteja prevista pelo fabricante na avaliação dos riscos inicial e que possa implicar que deixem de cumprir os requisitos essenciais de cibersegurança pertinentes, a modificação deverá ser considerada substancial. Por exemplo, as reparações podem ser equiparadas a operações de manutenção, desde que não modifiquem um produto com elementos digitais já colocado no mercado de tal maneira que possam afetar a conformidade com os requisitos aplicáveis ou alterar a finalidade prevista para a qual o produto foi avaliado.

(39) Tal como acontece com as reparações ou modificações físicas, um produto com elementos digitais deverá ser considerado substancialmente modificado por uma alteração do *software* quando a atualização do *software* modificar a finalidade prevista desse produto e essas alterações não tiverem sido previstas pelo fabricante na avaliação dos riscos inicial, ou quando a natureza do perigo se tiver alterado, ou quando o nível de risco de cibersegurança tiver

aumentado devido à atualização do *software*, e a versão atualizada do produto seja disponibilizada no mercado. Uma atualização de segurança concebida para reduzir o nível de risco de cibersegurança de um produto com elementos digitais, que não altere a finalidade prevista de um produto com elementos digitais, não é considerada uma modificação substancial. Tal inclui, geralmente, situações em que a atualização de segurança implica apenas pequenos ajustamentos do código-fonte. Por exemplo, pode ser esse o caso quando uma atualização de segurança resolve uma vulnerabilidade conhecida, nomeadamente através da modificação de funções ou do desempenho de um produto com elementos digitais com o único objetivo de reduzir o nível de risco de cibersegurança. De igual modo, uma atualização menor de funcionalidades, tal como melhorias visuais ou a introdução de novos pictogramas ou de novas línguas na interface do utilizador, não deverá, em geral, ser considerada uma modificação substancial. Em contrapartida, sempre que uma atualização de características modifique as funções inicialmente previstas ou o tipo ou desempenho de um produto com elementos digitais e cumpra os critérios acima referidos, deverá ser considerada uma modificação substancial, uma vez que a adição de novas características conduz, normalmente, a uma superfície de ataque mais ampla, aumentando, assim, o risco de cibersegurança. Por exemplo, pode ser esse o caso quando é aditado um novo elemento de entrada a uma aplicação, exigindo que o fabricante assegure uma validação adequada da entrada de dados. Ao avaliar se uma atualização de uma característica é considerada uma modificação substancial, não é relevante saber se é apresentada como uma atualização separada ou em combinação com uma atualização de segurança. A Comissão deverá emitir orientações sobre a forma de determinar o que constitui uma modificação substancial.

(40) Tendo em conta a natureza iterativa do desenvolvimento de *software*, os fabricantes que tenham colocado no mercado versões subsequentes de um produto de *software* em resultado de uma modificação substancial subsequente desse produto deverão poder fornecer atualizações de segurança durante o período de apoio apenas para a versão do produto de *software* que tenham colocado no mercado pela última vez. Só deverão poder fazê-lo se os utilizadores das versões anteriores do produto em causa tiverem acesso gratuito à versão do produto colocada no mercado pela última vez e não incorrerem em custos adicionais para ajustar o ambiente de *hardware* ou de *software* em que operam o produto. Por exemplo, pode ser esse o caso quando uma atualização do sistema operativo de secretária não exige equipamento informático novo, como uma unidade central de processamento mais rápida ou mais memória. No entanto, o fabricante deverá continuar a cumprir, durante o período de apoio, outros requisitos de tratamento de vulnerabilidades, tais como a existência de uma política de divulgação coordenada de vulnerabilidades ou de medidas para facilitar a partilha de informações sobre potenciais vulnerabilidades em todas as versões substancialmente modificadas subsequentes do produto de *software* colocado no mercado. Os fabricantes deverão poder fornecer pequenas atualizações de segurança ou funcionalidades que não constituam uma modificação substancial apenas para a versão ou subversão mais recente de um produto de *software* que não tenha sido substancialmente modificado. Ao mesmo tempo, se um produto de *hardware*, como um telemóvel inteligente, não for compatível com a última versão do sistema operativo com que foi originalmente entregue, o fabricante deverá continuar a fornecer atualizações de segurança pelo menos para a última versão compatível do sistema operativo durante o período de apoio.

(41) Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, sempre que ocorra uma modificação substancial que possa afetar a conformidade de um produto com elementos digitais 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 a uma nova avaliação da conformidade. Se aplicável, caso o fabricante proceda a uma avaliação da conformidade que envolva terceiros, deverá notificar-lhes as alterações que possam conduzir a modificações substanciais.

(42) Se um produto com elementos digitais for objeto de «recondicionamento», «manutenção» e «reparação» na aceção do artigo 2.º, pontos 18, 19 e 20, do Regulamento (UE) 2024/1781 do Parlamento Europeu e do Conselho ([19]), tal não conduz necessariamente a uma modificação substancial do produto se, por exemplo, a finalidade e as funcionalidades previstas não forem alteradas e o nível de risco não for afetado. No entanto, a atualização de um produto com elemento digitais pelo fabricante pode conduzir a alterações na conceção e no desenvolvimento desse produto e, por conseguinte, afetar a sua finalidade prevista e a sua conformidade com os requisitos estabelecidos no presente regulamento.

(43) Os produtos com elementos digitais deverão ser considerados importantes 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 a uma função que implique um risco significativo de efeitos adversos quanto à sua intensidade e capacidade para perturbar, controlar ou causar danos a vários outros produtos com elementos digitais ou à saúde, segurança ou proteção dos seus utilizadores através de manipulação direta, como uma função central do sistema, incluindo a gestão de redes, o controlo das configurações, a virtualização ou o tratamento de dados pessoais. 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

([19]) Regulamento (UE) 2024/1781 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece um regime para a definição de requisitos de conceção ecológica dos produtos sustentáveis, altera a Diretiva (UE) 2020/1828 e o Regulamento (UE) 2023/1542 e revoga a Diretiva 2009/125/CE (JO L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

incidente pode também aumentar quando o produto desempenha essencialmente uma função do sistema central, incluindo a gestão de redes, o controlo das configurações, a virtualização ou o tratamento de dados pessoais.

(44) Determinadas categorias de produtos críticos com elementos digitais deverão ser objeto de procedimentos de avaliação da conformidade mais rigorosos, sem deixar de manter uma abordagem proporcionada. Para o efeito, os produtos importantes com elementos digitais deverão 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 importantes com elementos digitais da classe II pode ter impactos negativos mais graves do que um incidente que envolva produtos importantes com elementos digitais da classe I devido, por exemplo, à natureza da sua função relacionada com a cibersegurança ou ao desempenho de outra função que comporte um risco significativo de efeitos adversos. Como indicação desses impactos negativos mais graves, os produtos com elementos digitais da classe II podem desempenhar uma funcionalidade relacionada com a cibersegurança ou outra função que comporte um risco significativo de efeitos adversos mais elevados do que os enumerados na classe I, ou cumprir ambos os critérios acima referidos. Os produtos importantes com elementos digitais da classe II deverão, por conseguinte, ser objeto de um procedimento de avaliação da conformidade mais rigoroso.

(45) Os produtos importantes com elementos digitais referidos no presente regulamento deverão ser entendidos como os produtos cuja funcionalidade principal é a de uma categoria de produtos importantes com elementos digitais estabelecida no presente regulamento. Por exemplo, o presente regulamento estabelece categorias de produtos importantes com elementos digitais que são definidas de acordo com a sua funcionalidade principal como barreiras de proteção ou sistemas de deteção ou prevenção de intrusões pertencentes à classe II. Consequentemente, as barreiras de proteção e os sistemas de deteção ou prevenção de intrusões estão sujeitos a uma avaliação obrigatória da conformidade por terceiros. Não é este o caso de outros produtos com elementos digitais não classificados como produtos importantes com elementos digitais que possam integrar barreiras de proteção ou sistemas de deteção ou prevenção de intrusões. A Comissão deverá adotar um ato de execução para especificar a descrição técnica das categorias de produtos importantes com elementos digitais abrangidas pelas classes I e II estabelecidas no presente regulamento.

(46) As categorias de produtos críticos com elementos digitais estabelecidas no presente regulamento têm uma funcionalidade relacionada com a cibersegurança e desempenham uma função que comporta um risco significativo de efeitos adversos em termos da sua intensidade e capacidade para perturbar, controlar ou causar dano a um grande número de outros produtos com elementos digitais através de manipulação direta. Além disso, essas categorias de produtos com elementos digitais são consideradas dependências críticas para as entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555. As categorias de produtos críticos com elementos digitais estabelecidas num anexo do presente regulamento, devido à sua importância crítica, já utilizam amplamente várias formas de certificação e estão também abrangidas pelo sistema europeu de certificação da cibersegurança baseado em critérios comuns (EUCC) estabelecido no Regulamento de Execução (UE) 2024/482 da Comissão ([20]). Por conseguinte, a fim de assegurar uma adequada proteção comum da cibersegurança dos produtos críticos com elementos digitais na União, pode ser adequado e proporcionado sujeitar essas categorias de produtos, por meio de um ato delegado, à certificação europeia obrigatória da cibersegurança, caso já esteja em vigor um sistema europeu de certificação da cibersegurança pertinente que abranja esses produtos e tenha sido realizada pela Comissão uma avaliação do potencial impacto no mercado da certificação obrigatória prevista. Essa avaliação deverá ter em conta tanto o lado da oferta como o da procura, incluindo a questão de saber se existe procura suficiente dos produtos com elementos digitais em causa, tanto pelos Estados-Membros como pelos utilizadores, para que seja exigida a certificação europeia da cibersegurança, bem como as finalidades para as quais os produtos com elementos digitais se destinam a ser utilizados, incluindo as dependências críticas, relativamente aos mesmos, por parte das entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555. A avaliação deverá também analisar os potenciais efeitos da certificação obrigatória sobre a disponibilidade desses produtos no mercado interno e as capacidades e o estado de preparação dos Estados-Membros para a aplicação dos sistemas europeus de certificação da cibersegurança pertinentes.

(47) Os atos delegados que exijam uma certificação europeia obrigatória da cibersegurança deverão determinar os produtos com elementos digitais que têm a funcionalidade principal de uma categoria de produtos críticos com elementos digitais estabelecida no presente regulamento que devem ser sujeitos a certificação obrigatória, bem como o nível de garantia exigido, que deverá ser, pelo menos, «substancial». O nível de garantia exigido deverá ser proporcional ao nível de risco de cibersegurança associado ao produto com elementos digitais. Por exemplo, se o produto com elementos digitais tiver a funcionalidade principal de uma categoria de produtos críticos com

([20]) Regulamento de Execução (UE) 2024/482 da Comissão, de 31 de janeiro de 2024, que estabelece regras de execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho no respeitante à adoção do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

elementos digitais estabelecida no presente regulamento e se destinar a ser utilizado num ambiente sensível ou crítico, como os produtos destinados à utilização por parte das entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555, pode exigir o nível de garantia mais elevado.

(48) A fim de assegurar uma adequada proteção comum da cibersegurança na União dos produtos com elementos digitais que tenham a funcionalidade principal de uma categoria de produtos críticos com elementos digitais estabelecida no presente regulamento, a Comissão deverá também ficar habilitada a adotar atos delegados para alterar o presente regulamento, acrescentando ou retirando categorias de produtos críticos com elementos digitais para as quais os fabricantes possam ser obrigados a obter um certificado europeu de cibersegurança, ao abrigo de um sistema europeu de certificação da cibersegurança, nos termos do Regulamento (UE) 2019/881, a fim de demonstrar a conformidade com o presente regulamento. Pode ser acrescentada uma nova categoria de produtos críticos com elementos digitais a essas categorias se existir uma dependência crítica em relação aos mesmos por parte das entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555 ou, se forem afetados por incidentes ou quando contiverem vulnerabilidades exploradas, tal pode conduzir a perturbações em cadeias de abastecimento críticas. Ao avaliar a necessidade de acrescentar ou retirar categorias de produtos críticos com elementos digitais por meio de um ato delegado, a Comissão deverá poder ter em conta se os Estados-Membros identificaram, a nível nacional, os produtos com elementos digitais que têm um papel crítico para a resiliência das entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555 e que enfrentam cada vez mais ciberataques na cadeia de abastecimento, com potenciais efeitos perturbadores graves. Além disso, a Comissão deverá poder ter em conta os resultados da avaliação coordenada dos riscos de segurança das cadeias de abastecimento críticas a nível da União, realizada em conformidade com o artigo 22.º da Diretiva (UE) 2022/2555.

(49) A Comissão deverá assegurar que um vasto leque de partes interessadas pertinentes seja consultado de forma estruturada e regular quando da preparação das medidas de execução do presente regulamento. Tal deverá ser o caso, em especial, sempre que a Comissão avalie a necessidade de eventuais atualizações das listas de categorias de produtos importantes ou críticos com elementos digitais, sempre que os fabricantes pertinentes devam ser consultados e os seus pontos de vista tidos em conta para analisar os riscos de cibersegurança, bem como o equilíbrio entre os custos e os benefícios da designação dessas categorias de produtos como importantes ou críticos.

(50) 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 que não estejam sempre relacionados com a cibersegurança, mas que possam ser consequência de uma violação da segurança. Esses riscos deverão continuar a ser regulamentados por outra legislação de harmonização da União pertinente distinta do presente regulamento. Se não for aplicável outra legislação de harmonização da União distinta do presente regulamento, deverão estar sujeitos ao Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho ([21]). 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 (UE) 2023/988, o capítulo III, secção 1, os capítulos V e VII e os capítulos IX a XI do Regulamento (UE) 2023/988 deverão 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 distinta do presente regulamento, na aceção do artigo 3.º, ponto 27, do Regulamento (UE) 2023/988.

(51) Os produtos com elementos digitais classificados como sistemas de IA de risco elevado nos termos do artigo 6.º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho ([22]) abrangidos pelo âmbito de aplicação do presente regulamento deverão cumprir os requisitos essenciais de cibersegurança estabelecidos no presente regulamento. Quando esses sistemas de IA de risco elevado cumprem os requisitos essenciais de cibersegurança do presente regulamento, deverão ser considerados conformes com os requisitos de cibersegurança estabelecidos no artigo 15.º do Regulamento (UE) 2024/1689 contanto que esses requisitos estejam abrangidos pela declaração de conformidade UE ou partes da mesma emitida ao abrigo do presente regulamento. Para esse efeito, a avaliação dos riscos de cibersegurança associados a um produto com elementos digitais classificado como um sistema de IA de risco elevado, nos termos do Regulamento (UE) 2024/1689, que será tida em conta durante as fases de planeamento, conceção, desenvolvimento, produção, entrega e manutenção desse produto, conforme exigido pelo presente regulamento, deverá ter em conta os riscos para a ciber-resiliência de um sistema de IA no que diz respeito às tentativas de terceiros não autorizados de alterar a sua utilização, comportamento ou desempenho, incluindo

([21]) Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos, que altera o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho e a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho e que revoga a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho e a Diretiva 87/357/CEE do Conselho (JO L 135 de 23.5.2023, p. 1).

([22]) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

vulnerabilidades específicas da IA, como o envenenamento de dados ou ataques por agentes antagónicos, bem como, se for caso disso, os riscos para os direitos fundamentais, em conformidade com o Regulamento (UE) 2024/1689. No que diz respeito aos procedimentos de avaliação da conformidade relacionados com os requisitos essenciais de cibersegurança relativos a um produto com elementos digitais que seja abrangido pelo âmbito de aplicação do presente regulamento e classificado como um sistema de IA de risco elevado, as disposições pertinentes do artigo 43.º do Regulamento (UE) 2024/1689 deverão, em regra, aplicar-se em vez das disposições pertinentes do presente regulamento. No entanto, esta regra não deverá resultar na redução do nível de garantia necessário para os produtos críticos ou importantes com elementos digitais, tal como referidos no presente regulamento. Por conseguinte, em derrogação desta regra, os sistemas de IA de risco elevado abrangidos pelo âmbito de aplicação do Regulamento (UE) 2024/1689, também qualificados como produtos críticos ou importantes com elementos digitais, tal como referidos no presente regulamento, e aos quais se aplica o procedimento de avaliação da conformidade baseado no controlo interno referido no anexo VI do Regulamento (UE) 2024/1689 deverão ser sujeitos aos procedimentos previstos no presente regulamento em matéria de avaliação da conformidade, no que diz respeito aos requisitos essenciais de cibersegurança do presente regulamento. Neste caso, em relação aos demais aspetos abrangidos pelo Regulamento (UE) 2024/1689, deverão aplicar-se as disposições pertinentes em matéria de avaliação da conformidade com base no controlo interno estabelecidas no anexo VI desse regulamento.

(52) Para melhorar a segurança dos produtos com elementos digitais colocados no mercado interno, é necessário estabelecer requisitos essenciais de cibersegurança aplicáveis a esses produtos. Esses requisitos essenciais de cibersegurança não deverão prejudicar as avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas a nível da União previstas no artigo 22.º da Diretiva (UE) 2022/2555, 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 deverão 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 da Comissão ([23]), na avaliação coordenada dos riscos de cibersegurança das redes 5G da UE e no conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G acordado pelo grupo de cooperação, criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555.

(53) Os fabricantes de produtos abrangidos pelo âmbito de aplicação do Regulamento (UE) 2023/1230 do Parlamento Europeu e do Conselho ([24]) que sejam também produtos com elementos digitais na aceção do presente regulamento deverão cumprir tanto os requisitos essenciais de cibersegurança estabelecidos no presente regulamento como os requisitos essenciais de saúde e segurança estabelecidos no Regulamento (UE) 2023/1230. Os requisitos essenciais de cibersegurança estabelecidos no presente regulamento e determinados requisitos essenciais previstos no Regulamento (UE) 2023/1230 podem dar resposta a riscos de cibersegurança semelhantes. Por conseguinte, a conformidade com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento pode facilitar o cumprimento dos requisitos essenciais que também abrangem determinados riscos de cibersegurança, tal como estabelecidos no Regulamento (UE) 2023/1230, em especial os relativos à proteção contra a corrupção e à segurança e fiabilidade dos sistemas de comando estabelecidos nas secções 1.1.9 e 1.2.1 do anexo III do referido regulamento. Essas sinergias têm de ser demonstradas pelo fabricante, por exemplo, aplicando, quando disponíveis, normas harmonizadas ou outras especificações técnicas que abranjam os requisitos essenciais de cibersegurança pertinentes na sequência de uma avaliação dos riscos que abranja esses riscos de cibersegurança. O fabricante deverá igualmente seguir os procedimentos de avaliação da conformidade aplicáveis, estabelecidos no presente regulamento e no Regulamento (UE) 2023/1230. A Comissão e as organizações europeias de normalização, nos trabalhos preparatórios de apoio à aplicação do presente regulamento e do Regulamento (UE) 2023/1230 e dos processos de normalização conexos, deverão promover a coerência na forma como os riscos de cibersegurança devem ser avaliados e na forma como esses riscos devem ser abrangidos por normas harmonizadas no que diz respeito aos requisitos essenciais pertinentes. Em especial, a Comissão e as organizações europeias de normalização deverão ter em conta o presente regulamento na preparação e elaboração de normas harmonizadas para facilitar a aplicação do Regulamento (UE) 2023/1230 no que diz respeito, em especial, aos aspetos de cibersegurança relacionados com a proteção contra a corrupção e a segurança e fiabilidade dos sistemas de comando estabelecidos nas secções 1.1.9 e 1.2.1 do anexo III do referido regulamento. A Comissão deverá fornecer orientações para apoiar os fabricantes abrangidos pelo presente regulamento que estejam igualmente sujeitos ao Regulamento (UE) 2023/1230, em especial para facilitar a demonstração da conformidade com os requisitos essenciais pertinentes estabelecidos no presente regulamento e no Regulamento (UE) 2023/1230.

(54) A fim de garantir a segurança dos produtos com elementos digitais tanto no momento da sua colocação no mercado como durante o período de utilização prevista do produto com elementos digitais, 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 de

([23]) Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, Cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).
([24]) Regulamento (UE) 2023/1230 do Parlamento Europeu e do Conselho, de 14 de junho de 2023, relativo às máquinas e que revoga a Diretiva 2006/42/CE do Parlamento Europeu e do Conselho e a Diretiva 73/361/CEE do Conselho (JO L 165 de 29.6.2023, p. 1).

cibersegurança relativos ao tratamento de vulnerabilidades ao longo do período de apoio, os fabricantes deverão determinar que outros requisitos essenciais de cibersegurança relativos às propriedades do produto são relevantes para o tipo de produto com elementos digitais em causa. Para o efeito, os fabricantes deverão realizar uma avaliação dos riscos de cibersegurança associados a um produto com elementos digitais, a fim de identificar os riscos e os requisitos essenciais de cibersegurança pertinentes, de disponibilizar os respetivos produtos com elementos digitais sem quaisquer vulnerabilidades passíveis de ser exploradas conhecidas que possam ter um impacto na segurança desses produtos e de aplicar de forma correta normas harmonizadas, especificações comuns ou normas europeias ou internacionais adequadas.

(55) Sempre que determinados requisitos essenciais de cibersegurança não sejam aplicáveis a um produto com elementos digitais, o fabricante deverá incluir uma justificação clara na avaliação dos riscos de cibersegurança incluída na documentação técnica. Tal pode ser o caso quando um requisito essencial de cibersegurança é incompatível com a natureza de um produto com elementos digitais. Por exemplo, a finalidade prevista de um produto com elementos digitais pode exigir que o fabricante siga normas de interoperabilidade amplamente reconhecidas, mesmo que os seus elementos de segurança deixem de ser considerados de ponta. De igual modo, outra legislação da União exige que os fabricantes apliquem requisitos de interoperabilidade específicos. Caso um requisito essencial de cibersegurança não seja aplicável a um produto com elementos digitais, mas o fabricante tenha identificado riscos de cibersegurança relacionados com esse requisito essencial de cibersegurança, deverá tomar medidas para fazer face a esses riscos por outros meios, por exemplo, limitando a finalidade prevista do produto a ambientes de confiança ou informando os utilizadores sobre esses riscos.

(56) Uma das medidas mais importantes a tomar pelos utilizadores para proteger os seus produtos com elementos digitais de ciberataques é instalar as mais recentes atualizações de segurança disponíveis com a maior brevidade possível. Os fabricantes deverão, por conseguinte, conceber os seus produtos e criar processos para assegurar que os produtos com elementos digitais incluam funções que permitam a notificação, a distribuição, o descarregamento e a instalação de atualizações de segurança de forma automática, em especial no caso dos produtos de consumo. Deverão também prever a possibilidade de se aprovar o descarregamento e a instalação das atualizações de segurança como etapa final. Os utilizadores deverão manter a capacidade de desativar as atualizações automáticas, através de um mecanismo claro e de fácil utilização, apoiado por instruções claras sobre a forma como os utilizadores podem optar pela autoexclusão. Os requisitos relativos às atualizações automáticas previstos num anexo do presente regulamento não são aplicáveis aos produtos com elementos digitais destinados principalmente a ser integrados como componentes noutros produtos. Também não se aplicam a produtos com elementos digitais para os quais os utilizadores não esperam razoavelmente atualizações automáticas, incluindo produtos com elementos digitais destinados a serem utilizados em redes TIC profissionais, especialmente em ambientes críticos e industriais em que uma atualização automática possa causar perturbação nas atividades. Independentemente de um produto com elementos digitais ser concebido para receber ou não atualizações automáticas, o seu fabricante deverá informar os utilizadores sobre as vulnerabilidades e disponibilizar atualizações de segurança sem demora. Sempre que um produto com elementos digitais tenha uma interface de utilizador ou meios técnicos semelhantes que permitam uma interação direta com os seus utilizadores, o fabricante deverá utilizar essas funcionalidades para informar os utilizadores de que o seu produto com elementos digitais chegou ao termo do período de apoio. As notificações deverão limitar-se ao necessário para assegurar a receção eficaz destas informações e não deverão ter um impacto negativo na experiência do utilizador do produto com elementos digitais.

(57) A fim de melhorar a transparência dos processos de tratamento de vulnerabilidades e assegurar que os utilizadores não sejam obrigados a instalar novas atualizações de funcionalidades com o único objetivo de receber as mais recentes atualizações de segurança, os fabricantes deverão assegurar, sempre que tecnicamente viável, que as novas atualizações de segurança sejam fornecidas separadamente das atualizações de funcionalidades.

(58) A comunicação conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 20 de junho de 2023, intitulada «Estratégia Europeia de Segurança Económica», afirma que a União deve maximizar os benefícios da sua abertura económica, minimizando simultaneamente os riscos decorrentes das dependências económicas de fornecedores de alto risco, através de um quadro estratégico comum para a segurança económica da União. As dependências de fornecedores de alto risco de produtos com elementos digitais podem colocar um risco estratégico, que deve ser resolvido a nível da União, especialmente quando os produtos com elementos digitais se destinem a ser utilizados pelas entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555. Esses riscos podem estar associados, mas não limitados, à jurisdição aplicável ao fabricante, às características da sua propriedade empresarial e às ligações de controlo ao governo de um país terceiro onde está estabelecido, em particular sempre que um país terceiro se envolva em espionagem económica ou comportamento estatal irresponsável no ciberespaço e a sua legislação permita um acesso arbitrário a quaisquer tipos de operações ou dados empresariais, incluindo dados comercialmente sensíveis, e possa impor obrigações para fins de informação sem um sistema de equilíbrio de poderes democrático, mecanismos de supervisão, o respeito das garantias processuais ou o direito de recurso junto de um poder judicial independente. Ao determinar a importância de um risco de cibersegurança na aceção do presente regulamento, a Comissão e as autoridades de fiscalização do mercado, de acordo com as suas responsabilidades estabelecidas no presente regulamento, deverão também ter em conta

fatores de risco não técnicos, em especial os estabelecidos na sequência de avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas a nível da União, realizadas em conformidade com o artigo 22.º da Diretiva (UE) 2022/2555.

(59) A fim de garantir a segurança dos produtos com elementos digitais após a sua colocação no mercado, os fabricantes deverão determinar o período de apoio, que deverá refletir o tempo previsto para a utilização do produto com elementos digitais. Ao determinar um período de apoio, o fabricante deverá ter em conta, em especial, as expectativas razoáveis dos utilizadores, a natureza do produto, bem como a legislação pertinente da União que determina a vida útil dos produtos com elementos digitais. Os fabricantes deverão também poder ter em conta outros fatores pertinentes. Os critérios deverão ser aplicados de forma a assegurar a proporcionalidade na determinação do período de apoio. Mediante pedido, o fabricante deverá fornecer às autoridades de fiscalização do mercado as informações que foram tidas em conta para determinar o período de apoio de um produto com elementos digitais.

(60) O período de apoio durante o qual o fabricante assegura o tratamento eficaz das vulnerabilidades não deverá ser inferior a cinco anos, a menos que a vida útil do produto com elementos digitais seja inferior a cinco anos, caso em que o fabricante deverá assegurar o tratamento das vulnerabilidades durante esse período de vida. Sempre que seja razoável esperar que o produto com elementos digitais esteja a ser utilizado durante um período superior a cinco anos, como acontece frequentemente com componentes de *hardware* como placas-mãe ou microprocessadores, dispositivos de rede como encaminhadores, modems ou comutadores, bem como *software*, como sistemas operativos ou ferramentas de edição de vídeos, os fabricantes deverão assegurar períodos de apoio mais longos em conformidade. Em especial, os produtos com elementos digitais destinados a serem utilizados em contextos industriais, como os sistemas de controlo industrial, são com frequência utilizados durante períodos de tempo significativamente mais longos. Um fabricante só deverá poder definir um período de apoio inferior a cinco anos se tal for justificado pela natureza do produto com elementos digitais em causa e se se previr que esse produto seja utilizado durante menos de cinco anos, caso em que o período de apoio deverá corresponder ao tempo de utilização previsto. Por exemplo, a vida útil de uma aplicação de rastreio de contactos destinada a ser utilizada durante uma pandemia pode ser limitada à duração da pandemia. Além disso, algumas aplicações informáticas só podem, por natureza, ser disponibilizadas com base num modelo de subscrição, em especial quando a aplicação deixa de estar disponível para o utilizador e, por conseguinte, deixa de ser utilizada uma vez caducada a assinatura.

(61) Quando os produtos com elementos digitais atingem o final dos seus períodos de apoio, a fim de assegurar que as vulnerabilidades possam ser tratadas após o termo do período de apoio, os fabricantes deverão ponderar a possibilidade de divulgar o código-fonte desses produtos com elementos digitais a outras empresas que se comprometam a dar seguimento à prestação de serviços de tratamento de vulnerabilidades ou ao público. Sempre que os fabricantes divulguem o código-fonte a outras empresas, deverão poder proteger a propriedade do produto com elementos digitais e impedir a divulgação do código-fonte ao público, por exemplo através de disposições contratuais.

(62) A fim de assegurar que os fabricantes em toda a União determinam períodos de apoio semelhantes para produtos com elementos digitais comparáveis, o ADCO deverá publicar estatísticas sobre os períodos de apoio médios determinados pelos fabricantes para as categorias de produtos com elementos digitais e emitir orientações indicando períodos de apoio adequados para essas categorias. Além disso, a fim de assegurar uma abordagem harmonizada em todo o mercado interno, a Comissão deverá poder adotar atos delegados para especificar períodos mínimos de apoio para categorias específicas de produtos sempre que os dados fornecidos pelas autoridades de fiscalização do mercado sugiram que os períodos de apoio determinados pelos fabricantes não estão sistematicamente em conformidade com os critérios para determinar os períodos de apoio estabelecidos no presente regulamento ou que os fabricantes de diferentes Estados-Membros determinam injustificadamente diferentes períodos de apoio.

(63) Os fabricantes deverão criar um ponto de contacto único que permita aos utilizadores comunicar facilmente com eles, inclusive para efeitos de comunicação e receção de informações sobre as vulnerabilidades do produto com elemento digital. Deverão tornar o ponto de contacto único facilmente acessível aos utilizadores e indicar claramente a sua disponibilidade, mantendo esta informação atualizada. Sempre que os fabricantes optem por oferecer ferramentas automatizadas, por exemplo, caixas de conversação, deverão também disponibilizar um número de telefone ou outros meios digitais de contacto, como um endereço de correio eletrónico ou um formulário de contacto. O ponto de contacto único não deverá basear-se exclusivamente em ferramentas automatizadas.

(64) Os fabricantes deverão disponibilizar no mercado os seus produtos com elementos digitais com uma configuração segura por defeito e fornecer atualizações de segurança aos utilizadores a título gratuito. Os fabricantes só deverão poder desviar-se dos requisitos essenciais de cibersegurança no que diz respeito a produtos personalizados que sejam montados com um determinado fim para um determinado utilizador empresarial e se tanto o fabricante como o utilizador tiverem concordado explicitamente com um conjunto diferente de cláusulas contratuais.

(65) Os fabricantes deverão notificar simultaneamente, através da plataforma única de comunicação de informações, tanto a equipa de resposta a incidentes de segurança informática (CSIRT, do inglês «computer security incident response team») designada como coordenadora, como a ENISA, das vulnerabilidades ativamente exploradas contidas em produtos com elementos digitais, bem como dos incidentes graves com impacto na segurança desses produtos. As notificações deverão ser apresentadas utilizando o terminal de notificação eletrónica de uma CSIRT designada como coordenadora e deverão ser simultaneamente acessíveis à ENISA.

(66) Os fabricantes deverão notificar vulnerabilidades que estejam a ser ativamente exploradas para assegurar que as CSIRT designadas como coordenadoras e a ENISA têm uma panorâmica adequada dessas vulnerabilidades e recebem as informações necessárias ao desempenho das suas funções, tal como estabelecidas na Diretiva (UE) 2022/2555, e ao reforço do nível global de cibersegurança das entidades essenciais e importantes a que se refere o artigo 3.º da mesma diretiva, bem como de assegurar o funcionamento eficaz das autoridades de fiscalização do mercado. 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 deverá ser considerada uma ameaça ao funcionamento do mercado interno. A ENISA deverá, com o acordo do fabricante, divulgar as vulnerabilidades corrigidas na base de dados europeia de vulnerabilidades criada nos termos do artigo 12.º, n.º 2, da Diretiva (UE) 2022/2555. A base de dados europeia de vulnerabilidades ajudará os fabricantes a detetar vulnerabilidades passiveis de ser exploradas conhecidas, identificadas nos seus produtos, a fim de garantir a colocação de produtos seguros no mercado.

(67) Os fabricantes deverão também notificar a CSIRT designada como coordenadora e a ENISA de qualquer incidente grave com impacto na segurança do produto com elementos digitais. A fim de garantir que os utilizadores possam reagir rapidamente a incidentes graves com impacto na segurança dos seus produtos com elementos digitais, os fabricantes deverão 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 de cibersegurança o justifiquem.

(68) As vulnerabilidades ativamente exploradas dizem respeito aos casos em que um fabricante estabelece que uma violação da segurança que afeta os seus utilizadores ou quaisquer outras pessoas singulares ou coletivas resultou do facto de um agente mal-intencionado ter utilizado uma falha num dos produtos com elementos digitais disponibilizados no mercado pelo fabricante. Exemplos de tais vulnerabilidades podem ser insuficiências nas funções de identificação e autenticação de um produto. As vulnerabilidades detetadas sem intenção maliciosa para fins de ensaio, investigação, correção ou divulgação de boa-fé, com vista a promover a segurança ou a proteção do proprietário do sistema e dos seus utilizadores, não estão sujeitas a notificações obrigatórias. Por outro lado, os incidentes graves com impacto na segurança do produto com elementos digitais referem-se a situações em que um incidente de cibersegurança afeta os processos de desenvolvimento, produção ou manutenção do fabricante de tal forma que pode resultar num aumento do risco de cibersegurança para os utilizadores ou outras pessoas. Um incidente significativo desta natureza pode incluir uma situação em que um atacante conseguiu introduzir com êxito um código malicioso no canal de lançamento através do qual o fabricante lança atualizações de segurança para os utilizadores.

(69) A fim de assegurar que as notificações podem ser rapidamente divulgadas a todas as CSIRT pertinentes designadas como coordenadoras e de permitir que os fabricantes apresentem uma notificação única em cada fase do processo de notificação, a ENISA deverá criar uma plataforma única de comunicação de informações com terminais nacionais de notificação eletrónica. As operações quotidianas da plataforma única de comunicação de informações deverão ser geridas e mantidas pela ENISA. As CSIRT designadas como coordenadoras deverão informar as respetivas autoridades de fiscalização do mercado sobre as vulnerabilidades ou os incidentes notificados. A plataforma única de comunicação de informações deverá ser concebida de modo a assegurar a confidencialidade das notificações, em especial no que diz respeito às vulnerabilidades para as quais ainda não está disponível uma atualização de segurança. Além disso, a ENISA deverá estabelecer procedimentos para tratar as informações de forma segura e confidencial. Com base nas informações que recolhe, a ENISA deverá elaborar, de dois em dois anos, um relatório técnico sobre as tendências emergentes em matéria de riscos de cibersegurança em produtos com elementos digitais e apresentá-lo ao grupo de cooperação criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555.

(70) Em circunstâncias excecionais e, em especial, a pedido do fabricante, a CSIRT designada como coordenadora que recebeu inicialmente uma notificação deverá poder decidir adiar a sua divulgação às outras CSIRT pertinentes designadas como coordenadoras através da plataforma única de comunicação de informações, sempre que tal se justifique por motivos relacionados com a cibersegurança e por um período de tempo estritamente necessário. A CSIRT designada como coordenadora deverá informar imediatamente a ENISA da decisão de adiar a divulgação e dos motivos em que se baseia, bem como do momento em que tenciona efetuar essa divulgação. A Comissão deverá elaborar, através de um ato delegado, especificações sobre os termos e condições em que podem ser aplicados motivos relacionados com a cibersegurança e deverá cooperar com a rede de CSIRT criada nos termos do artigo 15.º da Diretiva (UE) 2022/2555 e com a ENISA na elaboração do projeto de ato delegado. Exemplos de motivos relacionados com a cibersegurança incluem um procedimento de divulgação coordenada de vulnerabilidades em curso ou situações em que se espera que um fabricante forneça uma medida de atenuação em breve e os riscos de cibersegurança de uma divulgação imediata através da plataforma única de notificação superam os seus benefícios. Se tal for solicitado pela CSIRT designada como coordenadora, a ENISA deverá poder apoiar essa CSIRT na aplicação

de motivos relacionados com a cibersegurança em relação ao adiamento da divulgação da notificação com base nas informações que a ENISA recebeu dessa CSIRT sobre a decisão de reter uma notificação por esses motivos relacionados com a cibersegurança. Além disso, em circunstâncias particularmente excecionais, a ENISA não deverá receber em simultâneo todos os pormenores de uma notificação de uma vulnerabilidade ativamente explorada. Pode ser esse o caso quando o fabricante assinala, na sua notificação, que a vulnerabilidade notificada foi ativamente explorada por um agente mal-intencionado e que, de acordo com as informações disponíveis, não foi explorada em nenhum outro Estado-Membro além do da CSIRT designada como coordenadora à qual o fabricante notificou a vulnerabilidade, quando qualquer nova divulgação imediata da vulnerabilidade notificada for suscetível de resultar no fornecimento de informações cuja divulgação seria contrária aos interesses essenciais desse Estado-Membro, ou quando a vulnerabilidade notificada representar um elevado risco iminente de cibersegurança decorrente de uma maior divulgação. Nesses casos, a ENISA só recebe acesso simultâneo às informações de que o fabricante efetuou uma notificação, informações gerais sobre o produto com elementos digitais em causa, informações sobre a natureza geral da exploração e informações sobre o facto de esses motivos de segurança terem sido invocados pelo fabricante e, por conseguinte, o conteúdo integral da notificação ser recusado. A notificação completa deverá então ser disponibilizada à ENISA e a outras CSIRT pertinentes designadas como coordenadoras quando a CSIRT designada como coordenadora que recebeu inicialmente a notificação concluir que esses motivos de segurança, refletindo circunstâncias particularmente excecionais, tal como estabelecidas no presente regulamento, deixaram de existir. Se a ENISA, com base nas informações disponíveis, considerar que existe um risco sistémico que afeta a segurança do mercado interno, a ENISA deverá recomendar à CSIRT destinatária que divulgue a notificação completa às outras CSIRT designadas como coordenadoras e à própria ENISA.

(71) Quando os fabricantes notificam uma vulnerabilidade ativamente explorada ou um incidente grave com impacto na segurança do produto com elementos digitais, deverão indicar quão sensíveis consideram ser as informações notificadas. A CSIRT designada como coordenadora que inicialmente recebe a notificação deverá ter em conta estas informações ao avaliar se a notificação dá origem a circunstâncias excecionais que justifiquem um atraso na divulgação da notificação às outras CSIRT pertinentes designadas como coordenadoras com base em motivos fundamentados relacionados com a cibersegurança. Deverá também ter em conta essas informações ao avaliar se a notificação de uma vulnerabilidade ativamente explorada dá origem a circunstâncias particularmente excecionais que justifiquem que a notificação completa não seja disponibilizada simultaneamente à ENISA. Por último, as CSIRT designadas como coordenadoras deverão poder ter em conta essas informações ao determinar medidas adequadas para atenuar os riscos decorrentes dessas vulnerabilidades e desses incidentes.

(72) A fim de simplificar a comunicação das informações exigidas ao abrigo do presente regulamento, tendo em conta outros requisitos complementares em matéria de comunicação de informações estabelecidos no direito da União, como o Regulamento (UE) 2016/679, o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho ([25]), a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([26]) e a Diretiva (UE) 2022/2555, bem como para reduzir os encargos administrativos para as entidades, os Estados-Membros são incentivados a ponderar a criação, a nível nacional, de pontos de entrada únicos para esses requisitos de comunicação de informações. A utilização desses pontos de entrada únicos para a notificação de incidentes de segurança nos termos do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE não deverá afetar a aplicação das disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE, em especial as relativas à independência das autoridades aí referidas. Ao criar a plataforma única de comunicação de informações referida no presente regulamento, a ENISA deverá ter em conta a possibilidade de os terminais nacionais de notificação eletrónica a que se refere o presente regulamento serem integrados nos pontos de entrada únicos nacionais que podem também integrar outras notificações exigidas ao abrigo do direito da União.

(73) Ao criar a plataforma única de comunicação de informações referida no presente regulamento e a fim de beneficiar da experiência passada, a ENISA deverá consultar outras instituições ou agências da União que gerem plataformas ou bases de dados sujeitas a requisitos de segurança rigorosos, como a Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA). A ENISA deverá igualmente analisar as potenciais complementaridades com as bases de dados europeias de vulnerabilidades criadas nos termos do artigo 12.º, n.º 2, da Diretiva (UE) 2022/2555.

(74) Os fabricantes e outras pessoas singulares e coletivas deverão poder notificar uma CSIRT designada como coordenadora ou a ENISA, a título voluntário, sobre qualquer vulnerabilidade contida num produto com elementos

([25]) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).

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

digitais, ciberameaças que possam afetar o perfil de risco de um produto com elementos digitais, qualquer incidente com impacto na segurança do produto com elementos digitais, bem como quase incidentes que pudessem ter resultado num incidente desse tipo.

(75) Os Estados-Membros deverão procurar resolver, na medida do possível, os problemas encontrados pelos peritos que investigam as vulnerabilidades, nomeadamente a sua potencial sujeição à responsabilidade penal, em conformidade com o direito nacional. Dado que as pessoas singulares e coletivas que investigam as vulnerabilidades podem, em alguns Estados-Membros, incorrer em responsabilidade penal e civil, os Estados-Membros são incentivados a adotar orientações sobre a não instauração de ações penais contra quem faz investigação no domínio da segurança da informação e uma isenção de responsabilidade civil para as suas atividades.

(76) Os fabricantes de produtos com elementos digitais deverão instituir políticas de divulgação coordenada de vulnerabilidades, a fim de facilitar a comunicação de vulnerabilidades por parte de pessoas singulares ou de entidades, quer diretamente ao fabricante, quer indiretamente e, sempre que solicitado de forma anónima, através de CSIRT designadas como coordenadoras para efeitos de divulgação coordenada de vulnerabilidades, em conformidade com o artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555. A política dos fabricantes em matéria de divulgação coordenada das vulnerabilidades deverá 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. Além disso, os fabricantes deverão também ponderar a publicação das suas políticas de segurança num formato legível por máquina. 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 deverão 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. Tal refere-se aos chamados «programas de recompensas por deteção de erros de programação».

(77) A fim de facilitar a análise de vulnerabilidades, os fabricantes deverão identificar e documentar os componentes contidos nos produtos com elementos digitais, nomeadamente através da elaboração de uma lista de materiais de *software* (LMS). Uma LMS pode fornecer aos fabricantes, compradores e operadores de *software* informações que melhoram a sua compreensão da cadeia de abastecimento, o que tem múltiplos benefícios, ajudando, em particular, os fabricantes e os utilizadores a detetar vulnerabilidades e riscos de cibersegurança conhecidos surgidos recentemente. É particularmente importante que os fabricantes assegurem que os seus produtos com elementos digitais não contenham componentes vulneráveis desenvolvidos por terceiros. Os fabricantes não deverão ser obrigados a tornar pública a LMS.

(78) Ao abrigo dos novos e complexos modelos de negócio associados às vendas em linha, uma empresa que opere em linha pode prestar uma variedade de serviços. Consoante a natureza dos serviços prestados em relação a um determinado produto com elementos digitais, a mesma entidade poderá inserir-se em diferentes categorias de modelos empresariais ou operadores económicos. Sempre que uma entidade preste exclusivamente serviços de intermediação em linha para um determinado produto com elementos digitais e seja um mero prestador de um mercado em linha, na aceção do artigo 3.º, n.º 14, do Regulamento (UE) 2023/988, não é considerada um operador económico na aceção do presente regulamento. Sempre que a mesma entidade seja um prestador de um mercado em linha e também atue como operador económico, na aceção do presente regulamento, para a venda de determinados produtos com elementos digitais, deverá estar sujeita às obrigações estabelecidas no presente regulamento no que diz respeito a esses produtos. A título de exemplo, se o prestador de um mercado em linha também distribui um produto com elementos digitais, seria, pois, considerado um distribuidor no que diz respeito à venda desse produto. Do mesmo modo, se a entidade em questão vende os seus próprios produtos de marca com elementos digitais, seria considerado um fabricante e teria, por conseguinte, de cumprir os requisitos aplicáveis aos fabricantes. Além disso, algumas entidades podem ser consideradas prestadores de serviços de execução na aceção do artigo 3.º, ponto 11, do Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho ([27]), se oferecem serviços dessa natureza. Tais casos devem ser avaliados individualmente. Em virtude do papel proeminente que desempenham na facilitação do comércio eletrónico, os mercados em linha deverão procurar cooperar com as autoridades de fiscalização do mercado dos Estados-Membros, de molde a contribuir para que os produtos com elementos digitais adquiridos através dos mercados em linha cumpram os requisitos de cibersegurança estabelecidos no presente regulamento.

(79) A fim de facilitar a avaliação da conformidade com os requisitos estabelecidos no presente regulamento, deverá existir uma presunção de conformidade relativamente aos produtos com elementos digitais que estejam em conformidade com as normas harmonizadas, que traduzam os requisitos essenciais de cibersegurança previstos no presente regulamento em especificações técnicas pormenorizadas e que sejam adotados nos termos do Regulamento

([27]) 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 (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 169 de 25.6.2019, p. 1).

(UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([28]). O referido regulamento prevê um procedimento para a apresentação de objeções às normas harmonizadas caso essas normas não satisfaçam plenamente os requisitos previstos no presente regulamento. O processo de normalização deverá assegurar uma representação equilibrada dos interesses e a participação efetiva das partes interessadas da sociedade civil, incluindo as organizações de consumidores. Deverão também ser tidas em conta as normas internacionais que estejam em consonância com o nível de proteção da cibersegurança visado pelos requisitos essenciais de cibersegurança estabelecidos no presente regulamento, a fim de agilizar a elaboração de normas harmonizadas e a aplicação do presente regulamento, bem como de facilitar o seu cumprimento por parte das empresas, em especial das microempresas, das pequenas e médias empresas e das empresas que operam a nível mundial.

(80) A elaboração em tempo oportuno de normas harmonizadas durante o período de transição para a aplicação do presente regulamento e a sua disponibilidade antes da data de aplicação do presente regulamento serão particularmente importantes para a aplicação efetiva do mesmo. Tal aplica-se, em particular, aos produtos importantes com elementos digitais que se inserem na classe I. A disponibilidade de normas harmonizadas permitirá que os fabricantes desses produtos realizem as avaliações da conformidade com recurso ao procedimento de controlo interno, evitando assim estrangulamentos e atrasos nas atividades dos organismos de avaliação da conformidade.

(81) O Regulamento (UE) 2019/881 estabelece um regime europeu para a certificação voluntária da cibersegurança para produtos de TIC, processos de TIC e serviços de TIC. Os sistemas europeus de certificação da cibersegurança proporcionam um quadro comum de confiança que permite a utilização, pelos utentes, dos produtos com elementos digitais que recaem no âmbito de aplicação do presente regulamento. O presente regulamento deverá, por conseguinte, 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 europeu de cibersegurança nos termos do Regulamento (UE) 2019/881 que tenha sido identificado pela Comissão num ato de execução estão conformes com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento, contanto que o certificado europeu de cibersegurança ou a declaração de conformidade, ou partes dos mesmos, abranjam esses requisitos. Deverá ser avaliada à luz do presente regulamento a necessidade de novos sistemas europeus de certificação da cibersegurança para produtos com elementos digitais, nomeadamente aquando da elaboração do programa de trabalho evolutivo, em conformidade com o Regulamento (UE) 2019/881. Sempre que se afigure necessário dispor de um novo sistema que abranja produtos com elementos digitais, nomeadamente para facilitar o cumprimento do presente regulamento, a Comissão pode solicitar à ENISA que elabore projetos de sistema, em conformidade com o artigo 48.º do Regulamento (UE) 2019/881. Esses futuros sistemas europeus de certificação da cibersegurança que abranjam produtos com elementos digitais deverão ter em conta os requisitos essenciais de cibersegurança e os procedimentos de avaliação da conformidade estabelecidos no presente regulamento e facilitar o cumprimento do presente regulamento. Os sistemas europeus de certificação da cibersegurança que entrem em vigor antes da entrada em vigor do presente regulamento, podem necessitar de especificações adicionais sobre determinados aspetos das modalidades de aplicação da presunção de conformidade. A Comissão deverá ficar habilitada, por meio de atos delegados, a especificar as condições em que os sistemas europeus de certificação da cibersegurança podem ser utilizados para demonstrar a conformidade com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento. Ademais, a fim de evitar encargos administrativos indevidos, os fabricantes não deverão ser obrigados a assegurar a realização de uma avaliação da conformidade por terceiros prevista no Regulamento para os requisitos correspondentes, caso tenha sido emitido, ao abrigo desses sistemas europeus de certificação da cibersegurança, um certificado europeu de cibersegurança com um nível de garantia, no mínimo, correspondente a «substancial».

(82) Após a entrada em vigor do Regulamento de Execução (UE) 2024/482, que diz respeito aos produtos abrangidos pelo âmbito de aplicação do presente regulamento, tais como módulos de segurança físicos e microprocessadores, a Comissão deverá poder especificar, por meio de um ato delegado, de que forma o EUCC confere uma presunção de conformidade com os requisitos essenciais de cibersegurança a que se refere o anexo I do presente regulamento ou partes dos mesmos. Além disso, esse ato delegado 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 nos termos do presente regulamento para os requisitos correspondentes.

(83) O atual regime da normalização europeia, que se baseia nos princípios da «nova abordagem» estabelecidos na Resolução do Conselho, de 7 de maio de 1985, relativa a uma nova abordagem em matéria de harmonização técnica e de normalização, bem como no Regulamento (UE) n.º 1025/2012, constitui automaticamente o regime para elaborar normas que estabeleçam uma presunção da conformidade com os requisitos pertinentes essenciais de cibersegurança estabelecidos no presente regulamento. As normas europeias deverão ser orientadas para o mercado, tendo em conta o interesse público, assim como os objetivos estratégicos enunciados claramente no pedido dirigido pela Comissão a uma ou mais organizações europeias de normalização para que elaborem normas harmonizadas, dentro do prazo fixado, e deverão assentar num consenso. Contudo, na falta de referências pertinentes a normas

([28]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

harmonizadas, a Comissão deverá poder adotar atos de execução que estabeleçam especificações comuns para os requisitos essenciais de cibersegurança estabelecidos no presente regulamento, desde que o faça no devido respeito do papel e das funções da organização europeia de normalização, enquanto solução de recurso excecional para facilitar o cumprimento, pelo fabricante, da sua obrigação de observar os requisitos essenciais de cibersegurança em questão, quer quando o processo de normalização se encontra bloqueado, quer quando se verificam atrasos no estabelecimento de normas harmonizadas adequadas. Se esses atrasos se deverem à complexidade técnica da norma em questão, a Comissão deverá tomar esse facto em consideração antes de ponderar o estabelecimento de especificações comuns.

(84) A fim de estabelecer, da forma mais eficiente possível, especificações comuns aplicáveis aos requisitos essenciais de cibersegurança estabelecidos no presente regulamento, a Comissão deverá associar as partes interessadas ao processo.

(85) Para efeitos da publicação das referências às normas harmonizadas no *Jornal Oficial da União Europeia* em conformidade com o Regulamento (UE) n.º 1025/2012, entende-se por «período razoável» o período em que se prevê que prevista a referência à norma seja publicada no *Jornal Oficial da União Europeia*, a sua retificação ou a sua alteração e que não deverá exceder um ano após o prazo para a elaboração de uma norma europeia, fixado em conformidade com o Regulamento (UE) n.º 1025/2012.

(86) A fim de facilitar a avaliação da conformidade com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento, deverá 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.

(87) A aplicação de normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança adotados nos termos do Regulamento (UE) 2019/881 que estabeleçam uma presunção de conformidade em relação aos requisitos essenciais de cibersegurança aplicáveis aos produtos com elementos digitais facilitará a avaliação da conformidade pelos fabricantes. Se, em relação a determinados requisitos, o fabricante optar por não aplicar essas modalidades, deverá indicar, na sua documentação técnica, de que outro modo a conformidade é alcançada. Além disso, a aplicação de normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança adotados nos termos do Regulamento (UE) 2019/881 que estabeleçam uma presunção de conformidade dos fabricantes facilitaria a verificação, pelas autoridades de fiscalização do mercado, da conformidade dos produtos com elementos digitais. Assim sendo, incentiva-se os fabricantes de produtos com elementos digitais a aplicar essas normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança.

(88) Os fabricantes deverão 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 de cibersegurança estabelecidos no presente regulamento e, sendo caso disso, de outra legislação de harmonização da União aplicável ao produto com elementos digitais. Os fabricantes também podem ser obrigados a elaborar uma declaração de conformidade UE por outros atos jurídicos da União. Para assegurar o acesso efetivo à informação para efeitos de fiscalização do mercado, deverá ser elaborada uma declaração de conformidade UE única respeitante ao cumprimento de todos os atos jurídicos da União aplicáveis. A fim de reduzir os encargos administrativos que recaem sobre os operadores económicos, essa declaração de conformidade UE única deverá poder ser constituída por um dossiê que contenha as várias declarações de conformidade pertinentes.

(89) 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 ([29]). O presente regulamento deverá definir as regras que regem a aposição da marcação CE nos produtos com elementos digitais. A marcação CE deverá ser a única que garante que os produtos com elementos digitais cumprem os requisitos estabelecidos no presente regulamento.

(90) A fim de permitir que os operadores económicos demonstrem a conformidade com os requisitos essenciais de cibersegurança 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 ([30])

([29]) 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).

([30]) 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).

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 de cibersegurança estabelecidos no presente regulamento deverão basear-se nesses módulos. Os procedimentos de avaliação da conformidade deverão 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 com elementos digitais.

(91) A avaliação da conformidade dos produtos com elementos digitais que não constem da lista dos produtos importantes ou críticos com elementos digitais do presente regulamento pode ser realizada, regra geral, pelo fabricante sob a sua própria responsabilidade, de acordo com o procedimento de controlo interno baseado no módulo A da Decisão 768/2008/CE, em conformidade com o presente regulamento. Esta disposição aplica-se também aos casos em que um fabricante opte por não aplicar, total ou parcialmente, uma norma harmonizada, uma especificação comum ou um sistema europeu de certificação da cibersegurança aplicáveis. O fabricante dispõe de flexibilidade para escolher um procedimento de avaliação da conformidade mais rigoroso que envolva terceiros. No âmbito do procedimento de controlo interno de avaliação, o fabricante garante e declara, sob a sua exclusiva responsabilidade, que o produto com elementos digitais e os processos do fabricante cumprem os requisitos essenciais de cibersegurança aplicáveis estabelecidos no presente regulamento. Se um produto importante com elementos digitais for abrangido pela classe I, é obrigatória uma garantia adicional para demonstrar a conformidade com os requisitos essenciais de cibersegurança estabelecidos no presente regulamento. O fabricante deverá aplicar normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança adotados 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 europeus de certificação da cibersegurança, o fabricante deverá ser objeto de uma avaliação da conformidade por terceiros (com base nos módulos B e C ou no módulo H). 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 e C ou no módulo H da Decisão n.º 768/2008/CE foram escolhidos como sendo os mais adequados para avaliar a conformidade dos produtos importantes 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 produto importantes com elementos digitais abrangidos pela classe II, a avaliação da conformidade destes produtos deverá sempre envolver terceiros, mesmo se o produto estiver em conformidade total ou parcial com as normas harmonizadas, as especificações comuns ou os sistemas europeus de certificação da cibersegurança. Os fabricantes de produtos importantes com elementos digitais considerados *software* livre e de código-fonte aberto deverão poder seguir o procedimento de controlo interno baseado no módulo A, desde que divulguem publicamente a documentação técnica.

(92) 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. Essas atividades deverão 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 de cibersegurança estabelecidos no presente regulamento nas fases de conceção, desenvolvimento e produção.

(93) No que diz respeito às microempresas e às pequenas empresas, a fim de assegurar a proporcionalidade, é conveniente reduzir os custos administrativos, sem afetar o nível de proteção da cibersegurança dos produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento nem as condições de concorrência equitativas entre os fabricantes. Por conseguinte, é conveniente que a Comissão estabeleça um formulário simplificado de documentação técnica que vá ao encontro das necessidades das microempresas e das pequenas empresas. O formulário simplificado de documentação técnica adotado pela Comissão deverá abranger todos os elementos aplicáveis relacionados com a documentação técnica previstos no presente regulamento, tais como a descrição da conceção, do desenvolvimento e da produção do produto com elementos digitais, e especificar de que modo uma microempresa ou uma pequena empresa pode fornecer os elementos solicitados de forma concisa. Deste modo, o formulário contribuiria para aliviar os encargos administrativos em matéria de conformidade, proporcionando às empresas em causa segurança jurídica quanto à extensão e ao grau de pormenor das informações a fornecer. As microempresas e as pequenas empresas deverão poder optar por fornecer os elementos aplicáveis relacionados com a documentação técnica de forma elaborada, e não tirar partido do formulário técnico simplificado colocado à sua disposição.

(94) A fim de promover e proteger a inovação, é importante ter especialmente em conta os interesses dos fabricantes que sejam microempresas ou pequenas e médias empresas, em especial das microempresas e das pequenas empresas, incluindo as empresas em fase de arranque. Para o efeito, os Estados-Membros podem criar iniciativas destinadas aos fabricantes que sejam microempresas ou pequenas empresas, nomeadamente no domínio da formação, sensibilização, comunicação de informações e ensaios e atividades de avaliação da conformidade por terceiros, bem como estabelecer ambientes de testagem. Os custos de tradução relacionados com a documentação obrigatória, como a documentação técnica e as informações e instruções ao utilizador exigidas nos termos do presente regulamento, bem como a comunicação com as autoridades, podem constituir um custo significativo para os fabricantes, em especial os de menor dimensão. Por conseguinte, os Estados-Membros podem ponderar a possibilidade de uma das línguas por eles estabelecida ou aceite para efeitos de elaboração da documentação pelos fabricantes e de comunicação com os fabricantes ser uma língua amplamente compreendida pelo maior número possível de utilizadores.

(95) A fim de assegurar a aplicação harmoniosa do presente regulamento, os Estados-Membros deverão, antes da data de aplicação do presente regulamento, procurar garantir a disponibilidade de um número suficiente de organismos notificados na União para a realização de avaliações da conformidade. A Comissão deverá procurar assistir os Estados-Membros e outras partes pertinentes neste esforço, a fim de evitar estrangulamentos e obstáculos à entrada de fabricantes no mercado. As atividades de formação específicas conduzidas pelos Estados-Membros, nomeadamente com o apoio da Comissão, se for caso disso, podem contribuir para a disponibilidade de profissionais qualificados, designadamente para apoiar as atividades dos organismos notificados ao abrigo do presente regulamento. Além disso, tendo em conta os custos que a avaliação da conformidade por terceiros pode implicar, deverá ponderar-se o lançamento de iniciativas de financiamento a nível da União e nacional que visem reduzir esses custos para as microempresas e as pequenas empresas.

(96) A fim de assegurar a proporcionalidade, os organismos de avaliação da conformidade deverão, aquando da determinação das taxas aplicáveis aos procedimentos de avaliação da conformidade, ter em conta os interesses e necessidades específicos das microempresas e das pequenas e médias empresas, incluindo as empresas em fase de arranque. Em especial, os organismos de avaliação da conformidade deverão aplicar o procedimento de exame e proceder aos ensaios pertinentes previstos no presente regulamento apenas quando tal se afigure adequado e seguindo uma abordagem baseada no risco.

(97) Os ambientes de testagem da regulamentação deverão ter como objetivo promover a inovação e a competitividade das empresas, criando ambientes de ensaio controlados antes de os produtos com elementos digitais serem colocados no mercado. Os ambientes de testagem da regulamentação deverão contribuir para melhorar a segurança jurídica de todos os intervenientes abrangidos pelo âmbito de aplicação do presente regulamento, bem como facilitar e acelerar o acesso ao mercado da União de produtos com elementos digitais, em especial quando fornecidos por microempresas e pequenas empresas, incluindo empresas em fase de arranque.

(98) Para efeitos de avaliação da conformidade dos produtos com elementos digitais por terceiros, as autoridades notificadoras nacionais deverão 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.

(99) 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 deverá 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, deverá ser igualmente utilizada para efeitos de notificação.

(100) Os organismos de avaliação da conformidade que tenham sido acreditados e notificados ao abrigo do direito da União que estabelece requisitos semelhantes aos estabelecidos no presente regulamento – como, por exemplo, um organismo de avaliação da conformidade que tenha sido notificado no âmbito de um sistema europeu de certificação da cibersegurança adotado nos termos do Regulamento (UE) 2019/881 ou notificado ao abrigo do Regulamento Delegado (UE) 2022/30 –, deverão ser objeto de nova avaliação e notificados ao abrigo do presente regulamento. No entanto, as autoridades competentes podem definir sinergias no que diz respeito a eventuais sobreposições de requisitos, a fim de evitar encargos financeiros e administrativos desnecessários e assegurar um processo de notificação harmonioso e atempado.

(101) Uma acreditação organizada de forma transparente nos termos do Regulamento (CE) n.º 765/2008, que garanta a necessária confiança nos certificados de conformidade, deverá 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 deverão 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.

(102) 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 subcontratados e filiais que efetuam a avaliação da conformidade cumpram requisitos idênticos aos dos organismos notificados relativamente ao desempenho de tarefas de avaliação da conformidade.

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

(104) Uma vez que 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.

(105) 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.

(106) A fiscalização do mercado é um instrumento essencial para garantir a aplicação correta e uniforme do direito da União. Convém, pois, criar um regime 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, aplicam-se aos produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento.

(107) Em conformidade com o Regulamento (UE) 2019/1020, uma autoridade de fiscalização do mercado procede à fiscalização do mercado no território do Estado-Membro que a designou. O presente regulamento não deverá impedir os Estados-Membros de escolherem as autoridades competentes para desempenhar as atividades de fiscalização do mercado. Cada Estado-Membro deverá designar uma ou mais autoridades de fiscalização do mercado no seu território. Os Estados-Membros deverão poder optar por designar qualquer autoridade existente ou nova para atuar como autoridade de fiscalização do mercado, incluindo as autoridades competentes designadas ou criadas nos termos do artigo 8.º da Diretiva (UE) 2022/2555, as autoridades nacionais de certificação da cibersegurança designadas nos termos do artigo 58.º do Regulamento (UE) 2019/881, ou as autoridades de fiscalização do mercado designadas para efeitos da Diretiva 2014/53/UE. Os operadores económicos deverão cooperar plenamente com as autoridades de fiscalização do mercado e outras autoridades competentes. Cada Estado-Membro deverá informar a Comissão e os outros Estados-Membros sobre as suas autoridades de fiscalização do mercado e respetivos domínios de competência e deverá 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 deverá 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.

(108) Deverá ser criado um ADCO específico para a ciber-resiliência dos produtos com elementos digitais com vista à aplicação uniforme do presente regulamento, nos termos do artigo 30.º, n.º 2, do Regulamento (UE) 2019/1020. Este grupo ADCO deverá incluir representantes das autoridades de fiscalização do mercado designadas e, se for caso disso, representantes dos serviços de ligação únicos. A Comissão deverá apoiar e incentivar a cooperação entre as autoridades de fiscalização do mercado através da rede da União para a conformidade dos produtos, criada nos termos do 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 referido Regulamento, e um perito nacional facultativo, os presidentes dos ADCO e representantes da Comissão. A Comissão deverá participar nas reuniões da rede da União para a conformidade dos produtos, dos seus subgrupos e do respetivo ADCO. Deverá igualmente prestar assistência a este ADCO através de um secretariado executivo que faculte apoio técnico e logístico. O ADCO pode igualmente convidar peritos independentes a participar, bem como estabelecer contactos com outros ADCO, como os estabelecidos ao abrigo da Diretiva 2014/53/UE.

(109) As autoridades de fiscalização do mercado deverão cooperar estreitamente por intermédio dos ADCO estabelecidos ao abrigo do presente regulamento e deverão poder elaborar documentos de orientação para facilitar as atividades de fiscalização do mercado a nível nacional, nomeadamente estabelecendo boas práticas e indicadores para verificar de forma eficaz a conformidade dos produtos com elementos digitais com o presente regulamento.

(110) A fim de assegurar medidas oportunas, proporcionadas e eficazes em relação a produtos com elementos digitais que apresentem um risco de cibersegurança significativo, deverá prever-se um procedimento de salvaguarda da União no âmbito do qual as partes interessadas sejam informadas das medidas previstas para esses produtos. Tal deverá 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 deverá ser necessária qualquer outra intervenção da Comissão, salvo se a não conformidade puder ser imputada a deficiências de uma norma harmonizada.

(111) 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 a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555 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 deverão tomar medidas para exigir que o operador económico assegure que o produto deixe de apresentar esse risco ou que o recolha ou retire do mercado, consoante o risco. Assim que uma autoridade de fiscalização do mercado restrinja ou proíba a livre circulação de um produto com elementos digitais dessa forma, o Estado-Membro deverá 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 com elementos digitais que apresentem um risco, a Comissão deverá iniciar consultas com os Estados-Membros e o operador ou operadores económicos em causa e avaliar a medida nacional. Com base nos resultados desta avaliação, a Comissão deverá 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 operador ou operadores económicos em causa. Se se considerar que a medida é justificada, a Comissão também deverá ponderar a adoção de propostas de revisão do direito da União aplicável.

(112) No caso de produtos com elementos digitais que apresentem um risco de cibersegurança significativo, e sempre que existam motivos para crer que não cumprem o disposto no presente regulamento, ou de produtos que cumprem o disposto no presente regulamento, mas que apresentam outros riscos importantes, tais como riscos para a saúde ou a segurança das pessoas, para a observância das obrigações estabelecidas por força do direito da União ou do direito nacional que visa salvaguardar os direitos fundamentais ou para a disponibilidade, autenticidade, integridade ou confidencialidade dos serviços oferecidos com recurso a um sistema de informação eletrónico por entidades essenciais do tipo referido no artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555, a Comissão deverá poder solicitar à ENISA que realize uma avaliação. Com base nessa avaliação, a Comissão deverá poder adotar, por meio de atos de execução, medidas corretivas ou restritivas a nível da União, nomeadamente exigindo a retirada do mercado ou a recolha dos produtos com elementos digitais em causa, num prazo razoável e proporcional à natureza do risco. A Comissão deverá poder 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 do mercado não tiverem tomado medidas eficazes para corrigir a situação. Essas circunstâncias excecionais podem corresponder a situações de emergência em que, por exemplo, um produto com elementos digitais 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 (UE) 2022/2555, 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 deverá poder 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.

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

(114) As ações de controlo coordenadas simultâneas (ações de fiscalização conjuntas) são ações de execução específicas das autoridades de fiscalização do mercado que podem reforçar ainda mais a segurança dos produtos. Em especial, deverão 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 com elementos digitais apresentam frequentemente riscos de cibersegurança. Além disso, ao determinarem as categorias de produtos que deverão ser objeto de ações de fiscalização conjuntas, as autoridades de fiscalização do mercado deverão também ter em conta circunstâncias relacionadas com fatores de risco não técnicos. Para o efeito, as autoridades de fiscalização do mercado deverão poder ter em conta os resultados das avaliações coordenadas efetuadas a nível da União dos riscos de segurança das cadeias de abastecimento críticas, realizadas em conformidade com o artigo 22.º da Diretiva (UE) 2022/2555, incluindo circunstâncias relacionadas com fatores de risco não técnicos. A ENISA deverá apresentar às autoridades de fiscalização do mercado propostas de categorias de produtos com elementos digitais para as quais poderão ser organizadas ações de fiscalização conjuntas, com base, nomeadamente, nas notificações de vulnerabilidades de produtos e incidentes que recebe.

(115) Tendo em conta os seus conhecimentos especializados e o seu mandato, a ENISA deverá poder apoiar o processo de aplicação do presente regulamento. Em especial, a ENISA deverá 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 fiscalização conjuntas. Em circunstâncias excecionais, a ENISA deverá poder realizar, a pedido da Comissão, 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.

(116) O presente regulamento confere à ENISA determinadas atribuições que requerem recursos adequados, tanto em termos de conhecimentos especializados como de recursos humanos, para que a ENISA possa desempenhar essas atribuições de forma eficaz. A Comissão proporá os recursos orçamentais necessários para o quadro de pessoal da ENISA, em conformidade com o procedimento previsto no artigo 29.º do Regulamento (UE) 2019/881, aquando da elaboração do projeto de orçamento geral da União. Durante esse processo, a Comissão terá em conta os recursos globais da ENISA que lhe permitam exercer as suas atribuições, incluindo as conferidas à ENISA nos termos do presente regulamento.

(117) A fim de assegurar que o regime regulamentar possa ser adaptado sempre que necessário, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia (TFUE) deverá ser delegado na Comissão no que diz respeito a rever e incluir no anexo do presente regulamento os produtos importantes com elementos digitais. Deverá 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. Deverá também ser delegado na Comissão o poder de adotar atos nos termos desse artigo no que diz respeito à potencial obrigatoriedade de certificação ao abrigo de um sistema europeu de certificação dos produtos críticos com elementos digitais indicados no anexo do presente regulamento, bem como no que diz respeito à atualização da lista dos produtos críticos com elementos digitais com base nos critérios de criticidade estabelecidos no presente regulamento, e para 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 de cibersegurança ou partes dos mesmos, conforme estabelecidos no anexo do presente regulamento. Deverá igualmente ser delegado na Comissão o poder de adotar atos para especificar o período mínimo do apoio para categorias específicas de produtos relativamente às quais os dados de fiscalização do mercado apontam para a inadequação dos períodos de apoio, bem como para especificar os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações de vulnerabilidades ativamente exploradas. Além disso, deverá ser delegado na Comissão o poder de adotar atos para estabelecer programas voluntários de certificação de segurança destinados a avaliar a conformidade dos produtos com elementos digitais considerados *software* livre e de código-fonte aberto com todos ou com determinados requisitos essenciais de cibersegurança ou outras obrigações estabelecidas 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 às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([31]). Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados. O poder de adotar atos delegados é conferido à Comissão por um período de cinco anos a contar de 10 de dezembro de 2024. A Comissão deverá elaborar um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes deverá ser tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

(118) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão para especificar a descrição técnica das categorias de produtos importantes com elementos digitais estabelecidas num anexo do presente regulamento, especificar o formato e os elementos da lista de materiais do *software*, especificar mais pormenorizadamente o formato e o procedimento das notificações de vulnerabilidades ativamente exploradas e incidentes graves com impacto na segurança dos produtos com elementos digitais apresentadas pelos fabricantes, estabelecer especificações comuns abrangendo as exigências técnicas que possibilitem o cumprimento dos requisitos essenciais de cibersegurança estabelecidos no anexo I do presente regulamento, estabelecer especificações técnicas para os rótulos, os pictogramas ou quaisquer outras marcas relacionadas com a segurança dos produtos com elementos digitais, bem como os seus períodos de apoio e mecanismos para promover a sua utilização e aumentar a sensibilização do público para a segurança dos produtos com elementos digitais, especificar o formulário simplificado de documentação técnica tendo em conta as necessidades das microempresas e das pequenas empresas e decidir sobre medidas corretivas ou restritivas a nível da

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

União em circunstâncias excecionais que justifiquem uma intervenção imediata para preservar o bom funcionamento do mercado interno. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([32]).

(119) 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 deverão respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções.

(120) A fim de assegurar a aplicação efetiva das obrigações estabelecidas no presente regulamento, cada autoridade de fiscalização do mercado deverá ter poderes para impor ou solicitar a imposição de coimas. Por conseguinte, deverão 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, deverão ser tidas em conta todas as circunstâncias pertinentes da situação específica e, no mínimo, as explicitamente estabelecidas no presente regulamento, inclusive se o fabricante é uma microempresa ou uma pequena ou média empresa, nomeadamente uma empresa em fase de arranque, e se já foram aplicadas coimas pela mesma ou por outras autoridades de fiscalização do mercado ao mesmo operador económico por infrações semelhantes. As referidas circunstâncias poderiam ser agravantes, em situações em que a infração cometida pelo mesmo operador económico persista no território de outros Estados-Membros que não aquele em que já foi aplicada uma coima, ou atenuantes, para assegurar 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 deverá assegurar o respeito do princípio da proporcionalidade. Uma vez que as coimas não se aplicam a microempresas nem a pequenas empresas em caso de incumprimento do prazo de 24 horas para a notificação precoce de vulnerabilidades ativamente exploradas ou de incidentes graves com impacto na segurança do produto com elementos digitais, nem a administradores de *software* de código-fonte aberto em caso de infração ao presente regulamento, e sob reserva do princípio de que as sanções deverão ser efetivas, proporcionadas e dissuasivas, os Estados-Membros não deverão impor a essas entidades outro tipo de sanções de caráter pecuniário.

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

(122) Os Estados-Membros deverão analisar, tendo em conta as circunstâncias nacionais, a possibilidade de afetar as receitas provenientes das sanções previstas no presente regulamento, ou o seu equivalente financeiro, ao apoio às políticas de cibersegurança e para aumentar o nível de cibersegurança na União, nomeadamente através do aumento do número de profissionais qualificados no domínio da cibersegurança, reforçando as capacidades das microempresas e das pequenas e médias empresas e de uma maior sensibilização do público para as ciberameaças.

(123) Nas suas relações com países terceiros, a União 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. Esses 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 terceiros. Esses ARM são celebrados numa série de setores específicos, que podem variar de um país terceiro para outro. A fim de facilitar ainda mais o comércio, e reconhecendo que as cadeias de abastecimento de produtos com elementos digitais são 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 terceiros parceiros também é importante para reforçar a ciber-resiliência a nível mundial, uma vez que, a longo prazo, contribuirá para um regime de cibersegurança robustecido, tanto dentro como fora da União.

([32]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Os consumidores deverão poder fazer valer os seus direitos relativamente às obrigações impostas aos operadores económicos nos termos do presente regulamento através de ações coletivas em conformidade com a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho ([33]). Para o efeito, o presente regulamento deverá prever que a Diretiva (UE) 2020/1828 seja aplicável às ações coletivas relativas a infrações ao presente regulamento que prejudiquem ou possam prejudicar os interesses coletivos dos consumidores. Por conseguinte, o anexo I da referida diretiva deverá ser alterado em conformidade. Compete aos Estados-Membros assegurar que essas alterações se reflitam nas medidas de transposição adotadas nos termos dessa diretiva, embora a adoção das medidas de transposição nacionais a este respeito não constitua uma condição para a aplicabilidade da referida diretiva a essas ações coletivas. A aplicabilidade da referida diretiva às ações coletivas intentadas em relação a infrações às disposições do presente regulamento pelos operadores económicos que sejam ou possam ser lesivas dos interesses coletivos dos consumidores deverá ter início em 11 de dezembro de 2027.

(125) A Comissão deverá avaliar e reexaminar periodicamente o presente regulamento, em consulta com todas as partes interessadas pertinentes, nomeadamente para decidir sobre a eventual necessidade de o alterar à luz da evolução das condições sociais, políticas, tecnológicas ou do mercado. O presente regulamento facilitará o cumprimento das obrigações relacionadas com a segurança da cadeia de abastecimento por parte das entidades abrangidas pelo âmbito de aplicação do Regulamento (UE) 2022/2554 e da Diretiva (UE) 2022/2555 que utilizam produtos com elementos digitais. A Comissão deverá avaliar, no âmbito desse reexame periódico, os efeitos combinados do regime de cibersegurança da União.

(126) Os operadores económicos deverão dispor de tempo suficiente para se adaptarem aos requisitos previstos no presente regulamento. O presente regulamento deverá ser aplicável a contar de 11 de dezembro de 2027, com exceção das obrigações de comunicação de vulnerabilidades ativamente exploradas e incidentes graves com impacto na segurança dos produtos com elementos digitais, que deverão ser aplicáveis a contar de 11 de setembro de 2026 e das disposições sobre a notificação de organismos de avaliação da conformidade, que deverão ser aplicáveis a contar de 11 de junho de 2026.

(127) Importa apoiar as microempresas e as pequenas e médias empresas, inclusive as empresas em fase de arranque, no atinente à aplicação do presente regulamento e minimizar os riscos relativos à execução resultantes da falta de conhecimentos e competências especializadas no mercado, assim como para facilitar o cumprimento, por parte dos fabricantes, das obrigações que lhes incumbem por força do presente regulamento. O Programa Europa Digital e outros programas pertinentes da União prestam apoio financeiro e técnico que permite que essas empresas contribuam para o crescimento da economia da União e para o reforço do nível comum de cibersegurança na União. O Centro Europeu de Competências em Cibersegurança e os centros nacionais de coordenação, assim como os Polos Europeus de Inovação Digital criados pela Comissão e pelos Estados-Membros à escala da União ou no plano nacional, poderão também apoiar as empresas e as organizações do setor público e contribuir para a aplicação do presente regulamento. No âmbito das respetivas missões e domínios de competência, poderão prestar apoio técnico e científico às microempresas e às pequenas e médias empresas, designadamente no caso de atividades de ensaio e avaliações da conformidade por terceiros. Poderão também promover a utilização de instrumentos para facilitar a aplicação do presente regulamento.

(128) Além disso, os Estados-Membros deverão ponderar a adoção de medidas complementares destinadas a fornecer orientações e apoio às microempresas e às pequenas e médias empresas, nomeadamente através da criação de ambientes de testagem da regulamentação e canais de comunicação específicos. No intuito de reforçar o nível de cibersegurança na União, os Estados-Membros podem também considerar a possibilidade de prestar apoio com vista ao desenvolvimento de capacidades e competências relacionadas com a cibersegurança de produtos com elementos digitais, à melhoria da ciber-resiliência dos operadores económicos, mormente das microempresas e das pequenas e médias empresas, e à promoção da sensibilização do público para a cibersegurança dos produtos com elementos digitais.

(129) 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 esse objetivo.

(130) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([34]) e emitiu parecer em 9 de novembro de 2022 ([35]),

([33]) Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativa a ações coletivas para proteção dos interesses coletivos dos consumidores e que revoga a Diretiva 2009/22/CE (JO L 409 de 4.12.2020, p. 1).

([34]) 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).

([35]) JO C 452 de 29.11.2022, p. 23.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento estabelece o seguinte:

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

b) Requisitos essenciais de cibersegurança 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 de cibersegurança para os processos de tratamento de vulnerabilidades aplicados pelos fabricantes de modo a garantir a cibersegurança dos produtos com elementos digitais durante o período de utilização prevista dos produtos, bem como as obrigações dos operadores económicos em relação a esses processos;

d) Regras relativas à fiscalização do mercado, designadamente à supervisão, e à aplicação das regras e dos requisitos referidos no presente artigo.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento é aplicável aos produtos com elementos digitais disponibilizados no mercado cuja finalidade prevista ou utilização 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 jurídicos 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. O presente regulamento não é aplicável aos equipamentos abrangidos pelo âmbito de aplicação da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho ([36]).

5. 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 de cibersegurança previstos no anexo I pode ser limitada ou excluída, se:

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

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

A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º de forma a completar 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.

([36]) Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146).

6. O presente regulamento não se aplica às peças sobresselentes disponibilizadas no mercado para substituir componentes idênticos em produtos com elementos digitais e fabricadas de acordo com especificações iguais às dos componentes que se destinam a substituir.

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

8. As obrigações previstas no presente regulamento não implicam a prestação de informações cuja divulgação seja contrária aos interesses essenciais dos Estados-Membros no atinente à segurança nacional, à segurança pública ou à defesa.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Produto com elementos digitais», um produto de *software* ou *hardware* e as suas soluções de tratamento remoto de dados, incluindo componentes de *software* ou *hardware* que sejam colocados no mercado separadamente;

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

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

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

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

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

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

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

10) «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;

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

12) «Operador económico», o fabricante, o mandatário, o importador, o distribuidor ou outra pessoa singular ou coletiva sujeita a obrigações relacionadas com o fabrico de produtos com elementos digitais ou com a disponibilização de produtos com elementos digitais no mercado em conformidade com o presente regulamento;

13) «Fabricante», uma 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, monetizado ou gratuito;

14) «Administrador de *software* de código-fonte aberto», uma pessoa coletiva, que não um fabricante, cujo propósito ou objetivo consiste em prestar apoio sistemático e contínuo ao desenvolvimento de produtos específicos com elementos digitais que sejam considerados *software* livre e de código-fonte aberto e se destinem a atividades comerciais, e que garante a viabilidade desses produtos;

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

16) «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;

17) «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;

18) «Consumidor», uma pessoa singular que age com fins que não se incluam no âmbito da sua atividade comercial, empresarial, artesanal ou profissional;

19) «Microempresas», «pequenas empresas» e «médias empresas», microempresas, pequenas empresas e médias empresas, respetivamente, na aceção do anexo da Recomendação 2003/361/CE;

20) «Período de apoio», o período durante o qual um fabricante deve assegurar que as vulnerabilidades de um produto com elementos digitais são tratadas de forma eficaz e em conformidade com os requisitos essenciais de cibersegurança constantes da parte II do anexo I;

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

22) «Disponibilização no mercado», a 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;

23) «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;

24) «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;

25) «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;

26) «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 dos mesmos;

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

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

29) «Organismo notificado», um organismo de avaliação da conformidade designado nos termos do artigo 43.º ou de outra legislação de harmonização da União aplicável;

30) «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 de cibersegurança constantes da parte I do anexo I, ou que resulte numa modificação da finalidade prevista para a qual o produto com elementos digitais foi avaliado;

31) «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 de cibersegurança constantes do anexo I e de outra legislação de harmonização da União aplicável que preveja a sua aposição;

32) «Legislação de harmonização da União», legislação da União enumerada no anexo I do Regulamento (UE) 2019/1020 e qualquer outra legislação destinada a harmonizar as condições de comercialização dos produtos aos quais esse regulamento se aplica;

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

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

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

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

37) «Risco de cibersegurança», o potencial de perda ou perturbação causada por um incidente, expresso como uma combinação da magnitude dessa perda ou perturbação e da probabilidade de ocorrência do incidente;

38) «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;

39) «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;

40) «Vulnerabilidade», um ponto fraco, uma suscetibilidade ou uma falha de um produto com elementos digitais passível de ser explorado por uma ciberameaça;

41) «Vulnerabilidade passível de ser explorada», uma vulnerabilidade com potencial para ser efetivamente utilizada por um adversário em condições operacionais práticas;

42) «Vulnerabilidade ativamente explorada», uma vulnerabilidade relativamente à qual existem provas fiáveis da sua exploração num sistema por parte de um agente mal-intencionado sem a autorização do proprietário do sistema;

43) «Incidente», um incidente na aceção do artigo 6.º, ponto 6, da Diretiva (UE) 2022/2555;

44) «Incidente com impacto na segurança de um produto com elementos digitais», um incidente que afeta ou pode afetar negativamente a capacidade de um produto com elementos digitais de proteger a disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou das funções;

45) «Quase incidente», um quase incidente na aceção do artigo 6.º, ponto 5, da Diretiva (UE) 2022/2555;

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

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

48) «*Software* livre e de código-fonte aberto», *software* cujo código-fonte é partilhado abertamente e que é disponibilizado ao abrigo de uma licença gratuita e de código-fonte aberto que prevê todos os direitos para que o *software* seja livremente acessível, utilizável, modificável e redistribuível;

49) «Recolha», recolha na aceção do artigo 3.º, ponto 22, do Regulamento (UE) 2019/1020;

50) «Retirada», retirada na aceção do artigo 3.º, ponto 23, do Regulamento (UE) 2019/1020;

51) «CSIRT designada coordenadora», uma CSIRT designada coordenadora nos termos do artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555.

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, demonstrações ou eventos semelhantes, os Estados-Membros não podem impedir a apresentação ou utilização de um produto com elementos digitais que não cumpra o disposto no presente regulamento, designadamente dos seus protótipos, contanto que o produto seja apresentado com um sinal visível que indique nitidamente que o produto não cumpre o disposto no presente regulamento e que só será disponibilizado no mercado quando o cumprir.

3. Os Estados-Membros não podem impedir a disponibilização no mercado 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 com um sinal visível que 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.

4. O n.º 3 não se aplica aos componentes de segurança a que se refere a legislação de harmonização da União distinta do presente regulamento.

Artigo 5.º

Aquisição ou utilização de produtos com elementos digitais

1. O presente regulamento não impede os Estados-Membros de submeter os produtos com elementos digitais a requisitos adicionais de cibersegurança para a aquisição ou utilização desses produtos para fins específicos, inclusive quando esses produtos são adquiridos ou utilizados para fins de defesa ou segurança nacional, na condição de que esses requisitos sejam coerentes com as obrigações dos Estados-Membros estabelecidas no direito da União e sejam necessários e proporcionados para a consecução desses objetivos.

2. Sem prejuízo do disposto nas Diretivas 2014/24/UE e 2014/25/UE, sempre que sejam adquiridos produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento, os Estados-Membros devem velar por que o cumprimento dos requisitos essenciais de cibersegurança constantes do anexo I do presente regulamento, incluindo a capacidade dos fabricantes para lidar eficazmente com vulnerabilidades, seja tido em conta no processo de aquisição.

Artigo 6.º

Requisitos aplicáveis aos produtos com elementos digitais

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

a) Cumprirem os requisitos essenciais de cibersegurança constantes da parte I do anexo I, na condição de serem corretamente instalados, mantidos, utilizados para a respetiva finalidade prevista ou em condições razoavelmente previsíveis e, se for caso disso, de terem sido instaladas as atualizações de segurança necessárias; e

b) Os processos aplicados pelo fabricante cumprirem os requisitos essenciais de cibersegurança constantes da parte II do anexo I.

Artigo 7.º

Produtos importantes com elementos digitais

1. Os produtos com elementos digitais cuja funcionalidade principal seja a de uma categoria de produtos constante do anexo III são considerados produtos importantes com elementos digitais e estão sujeitos aos procedimentos de avaliação da conformidade a que se refere o artigo 32.º, n.ºs 2 e 3. Um produto com elementos digitais cuja funcionalidade principal seja a de uma categoria de produtos constante do anexo III que esteja integrado noutro produto com elementos digitais não implica, por si só, que o produto em que está integrado fique sujeito aos procedimentos de avaliação da conformidade a que se refere o artigo 32.º, n.ºs 2 e 3.

2. As categorias de produtos com elementos digitais a que se refere o n.º 1 do presente artigo, divididas nas classes I e II constantes do anexo III, satisfazem, pelo menos, um dos seguintes critérios:

a) O produto com elementos digitais desempenha essencialmente funções cruciais para a cibersegurança de outros produtos, redes ou serviços, como a proteção da autenticação e do acesso, a prevenção e deteção de intrusões, a segurança dos pontos terminais ou a proteção das redes;

b) O produto com elementos digitais desempenha uma função que acarreta um risco significativo de efeitos adversos quanto à sua intensidade e capacidade para perturbar, controlar ou causar danos a vários outros produtos ou à saúde, segurança ou proteção dos seus utilizadores através de manipulação direta, como uma função central do sistema, em particular a gestão de redes, o controlo das configurações, a virtualização ou o tratamento de dados pessoais.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º para alterar o anexo III incluindo na lista uma nova categoria em cada classe de categorias de produtos com elementos digitais e especificando a sua definição, movendo uma categoria de produtos de uma classe para outra ou retirando uma categoria existente. Ao avaliar a necessidade de alterar a lista estabelecida no anexo III, a Comissão deve ter em conta as funcionalidades relacionadas com a cibersegurança ou a função e o nível de risco de cibersegurança decorrente dos produtos com elementos digitais com base nos critérios a que se refere o n.º 2 do presente artigo.

Os atos delegados a que se refere o primeiro parágrafo do presente número preveem, se for caso disso, um período de transição mínimo de 12 meses, em especial se for aditada uma nova categoria de produtos importantes com elementos digitais à classe I ou II ou for transferida da classe I para a classe II constantes do anexo III, antes da aplicação dos procedimentos de avaliação da conformidade pertinentes a que se refere o artigo 32.º, n.ºs 2 e 3, salvo se, por imperativos de urgência, se justificar um período de transição mais curto.

4. Até 11 de dezembro de 2025, a Comissão adota um ato de execução com a descrição técnica das categorias de produtos com elementos digitais das classes I e II constantes do anexo III e a descrição técnica das categorias de produtos com elementos digitais constantes do anexo IV. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 62.º, n.º 2.

Artigo 8.º

Produtos críticos com elementos digitais

1. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º para completar o presente regulamento, com vista a determinar que produtos com elementos digitais cuja funcionalidade principal é a de uma categoria de produtos constante do anexo IV do presente regulamento devem obrigatoriamente obter um certificado europeu de cibersegurança com um nível de garantia pelo menos «substancial» ao abrigo de um sistema europeu de certificação da cibersegurança adotado nos termos do Regulamento (UE) 2019/881, no intuito de demonstrar a conformidade com os requisitos essenciais de cibersegurança definidos no anexo I do presente regulamento ou parte deles, na condição de que tenha sido adotado, nos termos do Regulamento (UE) 2019/881, um sistema europeu de certificação da cibersegurança que abranja essas categorias de produtos com elementos digitais e de que esse sistema esteja à disposição dos fabricantes. Os referidos atos delegados especificam o nível de garantia exigido, que deve ser proporcionado em relação ao nível de risco de cibersegurança associado aos produtos com elementos digitais e ter em conta a sua finalidade prevista, incluindo as dependências críticas em relação aos mesmos por parte das entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555.

Antes de adotar esses atos delegados, a Comissão procede a uma avaliação do potencial impacto das medidas previstas no mercado e consulta as partes interessadas pertinentes, inclusive o grupo europeu para a certificação da cibersegurança criado nos termos do Regulamento (UE) 2019/881. A avaliação deve ter em conta o grau de preparação e de capacidade dos Estados-Membros para a aplicação do sistema europeu de certificação da cibersegurança pertinente. Caso não tenham sido adotados os atos delegados a que se refere o primeiro parágrafo do presente número, os produtos com elementos digitais cuja funcionalidade principal seja a de uma categoria de produtos constante do anexo IV estão sujeitos aos procedimentos de avaliação da conformidade a que se refere o artigo 32.º, n.º 3.

Os atos delegados a que se refere o primeiro parágrafo preveem um período de transição mínimo de seis meses, salvo se, por imperativos de urgência, se justificar um período de transição mais curto.

2. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º para alterar o anexo IV aditando ou retirando categorias de produtos críticos com elementos digitais. Ao determinar tais categorias de produtos críticos com elementos digitais e o nível de garantia exigido, em conformidade com o n.º 1 do presente artigo, a Comissão deve ter em conta os critérios a que se refere o artigo 7.º, n.º 2, e assegurar que as categorias de produtos com elementos digitais cumpram pelo menos um dos seguintes critérios:

a) Existe uma dependência crítica das entidades essenciais a que se refere o artigo 3.º da Diretiva (UE) 2022/2555 em relação à categoria de produtos com elementos digitais;

b) Os incidentes e as vulnerabilidades exploradas relativos à categoria de produtos com elementos digitais poderiam provocar perturbações graves em cadeias de abastecimento críticas em todo o mercado interno.

Antes de adotar esses atos delegados, a Comissão procede a uma avaliação do tipo a que se refere o n.º 1.

Os atos delegados a que se refere o primeiro parágrafo preveem um período de transição mínimo de seis meses, salvo se, por imperativos de urgência, se justificar um período de transição mais curto.

Artigo 9.º

Consulta das partes interessadas

1. Ao preparar as medidas de execução do presente regulamento, a Comissão consulta e tem em conta os pontos de vista das partes interessadas pertinentes, como as autoridades competentes dos Estados-Membros, empresas do setor privado, nomeadamente microempresas e pequenas e médias empresas, a comunidade de *software* de código-fonte aberto, as associações de consumidores, o meio académico e as agências e organismos competentes da União, além de grupos de peritos criados à escala da União. Em particular, a Comissão, se for caso disso, consulta e recolhe de forma estruturada os pontos de vista dessas partes interessadas ao:

a) Elaborar as orientações a que se refere o artigo 26.º;

b) Elaborar as descrições técnicas das categorias de produtos constantes do anexo III em conformidade com o artigo 7.º, n.º 4, avaliar a necessidade de potenciais atualizações da lista de categorias de produtos em conformidade com o artigo 7.º, n.º 3, e o artigo 8.º, n.º 2, ou realizar a avaliação do potencial impacto no mercado a que se refere o artigo 8.º, n.º 1, sem prejuízo do disposto no artigo 61.º;

c) Levar a cabo trabalho preparatório para a avaliação e reexame do presente regulamento.

2. A Comissão organiza sessões periódicas de consulta e informação, pelo menos uma vez por ano, para recolher os pontos de vista das partes interessadas a que se refere o n.º 1 sobre a aplicação do presente regulamento.

Artigo 10.º

Reforço das competências num ambiente digital de ciber-resiliência

Para efeitos do presente regulamento e com vista a dar resposta às necessidades dos profissionais em apoio da aplicação do presente regulamento, os Estados-Membros, com o apoio da Comissão, do Centro Europeu de Competências em Cibersegurança e da ENISA, se for caso disso, no pleno respeito da responsabilidade dos Estados-Membros no domínio da educação, promovem medidas e estratégias destinadas a:

a) Desenvolver competências de cibersegurança e criar instrumentos organizacionais e tecnológicos para assegurar a disponibilidade de profissionais qualificados suficientes, no intuito de apoiar as atividades das autoridades de fiscalização do mercado e dos organismos de avaliação da conformidade;

b) Intensificar a colaboração entre o setor privado, os operadores económicos, nomeadamente através da requalificação ou da melhoria das competências dos trabalhadores dos fabricantes, dos consumidores, dos prestadores de serviços de formação e das administrações públicas, alargando, desta forma, as opções para os jovens acederem a empregos no setor da cibersegurança.

Artigo 11.º

Segurança geral dos produtos

Em derrogação do artigo 2.º, n.º 1, terceiro parágrafo, alínea b), do Regulamento (UE) 2023/988,o capítulo III, secção 1, os capítulos V e VII e os capítulos IX a XI desse regulamento aplicam-se aos produtos com elementos digitais no que respeita aos aspetos e riscos ou às categorias de riscos não abrangidos pelo presente regulamento nos casos em que esses produtos não estejam sujeitos a requisitos de segurança específicos estabelecidos noutra «legislação de harmonização da União», na aceção do artigo 3.º, ponto 27, do Regulamento (UE) 2023/988.

Artigo 12.º

Sistemas de IA de risco elevado

1. Sem prejuízo dos requisitos de exatidão e solidez previstos no artigo 15.º do Regulamento (UE) 2024/1689, os produtos com elementos digitais que sejam abrangidos pelo âmbito de aplicação do presente regulamento e que sejam classificados como sistemas de IA de risco elevado nos termos do artigo 6.º desse regulamento são considerados conformes com os requisitos de cibersegurança estabelecidos no artigo 15.º desse regulamento nos casos em que:

a) Esses produtos satisfazem os requisitos essenciais de cibersegurança constantes da parte I do anexo I;

b) Os processos aplicados pelo fabricante cumprem os requisitos essenciais de cibersegurança constantes da parte II do anexo I; e

c) A consecução do nível de proteção de cibersegurança exigido nos termos do artigo 15.º do Regulamento (UE) 2024/1689 é demonstrada na declaração UE de conformidade emitida ao abrigo do presente regulamento.

2. Os produtos com elementos digitais e os requisitos de cibersegurança referidos no n.º 1 do presente artigo estão sujeitos ao procedimento de avaliação da conformidade pertinente previsto no artigo 43.º do Regulamento (UE) 2024/1689. Para efeitos dessa avaliação, os organismos notificados competentes para verificar a conformidade dos sistemas de IA de risco elevado ao abrigo do Regulamento (UE) 2024/1689 são também competentes para 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 39.º do presente regulamento tenha sido avaliada no contexto do procedimento de notificação previsto no Regulamento (UE) 2024/1689.

3. Em derrogação do n.º 2 do presente artigo, os produtos importantes com elementos digitais enumerados no anexo III do presente regulamento que estejam sujeitos aos procedimentos de avaliação da conformidade referidos no artigo 32.º, n.º 2, alíneas a) e b), e no artigo 32.º, n.º 3, do presente regulamento e os produtos críticos com elementos digitais enumerados no anexo IV do presente regulamento que devem obter um certificado europeu de cibersegurança em conformidade com o artigo 8.º, n.º 1, do presente regulamento ou que, na sua ausência, estão sujeitos aos procedimentos de avaliação da conformidade a que se refere o artigo 32.º, n.º 3, do presente regulamento, que sejam classificados como sistemas de IA de risco elevado nos termos do artigo 6.º do Regulamento (UE) 2024/1689 e aos quais seja aplicável o procedimento de avaliação da conformidade baseado no controlo interno referido no anexo VI do (UE) 2024/1689, ficam sujeitos aos procedimentos de avaliação da conformidade previstos no presente regulamento no que diz respeito aos requisitos essenciais de cibersegurança nele previstos.

4. Os fabricantes de produtos com elementos digitais a que se refere o n.º 1 do presente artigo podem participar nos ambientes de testagem da regulamentação da IA a que se refere o artigo 57.º do Regulamento (UE) 2024/1689.

CAPÍTULO II

OBRIGAÇÕES DOS OPERADORES ECONÓMICOS E DISPOSIÇÕES EM RELAÇÃO AO *SOFTWARE* LIVRE E DE CÓDIGO-FONTE ABERTO

Artigo 13.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 de cibersegurança constantes da parte I do anexo I.

2. Para efeitos do cumprimento do 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 e minimizar os respetivos impactos, nomeadamente na saúde e segurança dos utilizadores.

3. A avaliação dos riscos de cibersegurança deve ser documentada e atualizada, conforme adequado, durante um período de apoio a determinar em conformidade com o n.º 8 do presente artigo. Essa avaliação dos riscos de cibersegurança deve incluir, pelo menos, uma análise dos riscos de cibersegurança com base na finalidade prevista e na utilização razoavelmente previsível, assim como nas condições de utilização do produto com elementos digitais, como o ambiente operacional ou os ativos a proteger, tendo em conta o período de utilização previsível do produto. A avaliação dos riscos de cibersegurança deve indicar se e, em caso afirmativo, de que forma, os requisitos de segurança constantes da parte I, ponto 2, do anexo I são aplicáveis ao produto com elementos digitais em causa e a forma como esses requisitos são aplicados com base na avaliação dos riscos de cibersegurança. Deve igualmente indicar a forma como o fabricante aplica a parte I, ponto 1, do anexo I e os requisitos de tratamento de vulnerabilidades constantes da parte II do anexo I.

4. Ao colocar um produto com elementos digitais no mercado, o fabricante deve incluir a avaliação dos riscos de cibersegurança a que se refere o n.º 3 do presente artigo na documentação técnica exigida nos termos do artigo 31.º e do anexo VII. Para os produtos com elementos digitais a que se refere o artigo 12.º, que também sejam abrangidos por outros atos jurídicos da União, a avaliação dos riscos de cibersegurança pode integrar a avaliação dos riscos exigida por esses atos jurídicos da União. Sempre que determinados requisitos essenciais de cibersegurança não sejam aplicáveis ao produto com elementos digitais, o fabricante deve incluir uma justificação clara para esse efeito na referida documentação técnica.

5. Para efeitos do cumprimento do n.º 1, os fabricantes devem exercer a diligência devida quando integram componentes provenientes de terceiros de modo que esses componentes não comprometam a cibersegurança do produto com elementos digitais, inclusivamente ao integrarem componentes de *software* livre e de código-fonte aberto que não tenham sido disponibilizados no mercado no decorrer de uma atividade comercial.

6. Ao identificarem uma vulnerabilidade num componente, incluindo num componente de código aberto, integrado num produto com elementos digitais, os fabricantes devem comunicar a vulnerabilidade à pessoa ou entidade responsável pelo fabrico ou pela manutenção do componente e tratar e corrigir a vulnerabilidade de acordo com os requisitos de tratamento de vulnerabilidades constantes da parte II do anexo I. Caso os fabricantes tenham desenvolvido uma modificação de *software* ou *hardware* para corrigir a vulnerabilidade desse componente, devem partilhar o código ou a documentação pertinente com a pessoa ou entidade responsável pelo fabrico ou pela manutenção do componente, se for caso disso num formato legível por máquina.

7. Os fabricantes devem documentar sistematicamente os aspetos de cibersegurança pertinentes respeitantes aos produtos com elementos digitais, de forma proporcional à sua natureza e aos riscos de cibersegurança, incluindo as vulnerabilidades de que tenham conhecimento e eventuais informações pertinentes comunicadas por terceiros, bem como, se for caso disso, atualizar a avaliação dos riscos de cibersegurança dos produtos.

8. Ao colocarem um produto com elementos digitais no mercado e durante o período de apoio, os fabricantes devem garantir que as vulnerabilidades desse produto, inclusive dos seus componentes, sejam tratadas de forma eficaz e em conformidade com os requisitos essenciais de cibersegurança constantes da parte II do anexo I.

Os fabricantes devem determinar o período de apoio de modo que reflita o período durante o qual se prevê que o produto seja utilizado, tendo em conta, em especial, as expectativas razoáveis dos utilizadores, a natureza do produto, incluindo a sua finalidade prevista, assim como a legislação pertinente da União que determina a vida útil dos produtos com elementos digitais. Ao determinarem o período de apoio, os fabricantes podem também ter em conta os períodos de apoio dos produtos com elementos digitais que oferecem uma funcionalidade semelhante colocados no mercado por outros fabricantes, a disponibilidade do ambiente operacional, os períodos de apoio dos componentes integrados que têm um papel essencial e provêm de terceiros, assim como as orientações pertinentes dadas pelo grupo de cooperação administrativa (ADCO) específico criado nos termos do artigo 52.º, n.º 15, e pela Comissão. Os aspetos a ter em conta para determinar o período de apoio devem ser considerados de um modo que garanta a proporcionalidade.

Sem prejuízo do disposto no segundo parágrafo, o período de apoio é de, pelo menos, cinco anos. Caso se preveja que o produto com elementos digitais seja utilizado durante menos de cinco anos, o período de apoio deve corresponder ao tempo de utilização previsto.

Tendo em conta as recomendações do ADCO a que se refere o artigo 52.º, n.º 16, a Comissão pode adotar atos delegados, nos termos do artigo 61.º, para completar o presente regulamento, especificando o período mínimo de apoio para categorias específicas de produtos sempre que os dados de fiscalização do mercado sugiram períodos de apoio inadequados.

Os fabricantes devem incluir, na documentação técnica, as informações que foram tidas em conta para determinar o período de apoio de um produto com elementos digitais em conformidade com o anexo VII.

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

9. Os fabricantes devem assegurar que cada uma das atualizações de segurança a que se refere a parte II, ponto 8, do anexo I que tenha sido disponibilizada aos utilizadores durante o período de apoio permaneça disponível após a sua emissão durante um período mínimo de 10 anos ou durante o restante período de apoio, consoante o que for mais longo.

10. Caso um fabricante tenha colocado no mercado versões posteriores de um produto de *software* substancialmente alteradas, esse fabricante pode garantir a conformidade com o requisito essencial de cibersegurança constante da parte II, ponto 2, do anexo I apenas relativamente à última versão que tiver colocado no mercado, desde que os utilizadores das versões anteriormente colocadas no mercado tenham acesso à última versão colocada no mercado a título gratuito e não incorram em custos adicionais para ajustar o ambiente de *hardware* e *software* em que utilizam a versão original desse produto.

11. Os fabricantes podem manter arquivos públicos de *software* que melhorem o acesso dos utilizadores às versões anteriores. Nesses casos, os utilizadores devem ser informados, de forma clara e facilmente acessível, sobre os riscos associados à utilização de *software* não abrangido pelo período de apoio.

12. Antes de colocarem um produto com elementos digitais no mercado, os fabricantes devem elaborar a documentação técnica referida no artigo 31.º.

Os fabricantes devem executar ou mandar executar os procedimentos de avaliação da conformidade escolhidos a que se refere o artigo 32.º.

Sempre que a conformidade do produto com elementos digitais com os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e dos processos aplicados pelo fabricante com os requisitos essenciais de cibersegurança constantes da parte II do anexo I, tenha sido demonstrada através desse procedimento de avaliação da conformidade, os fabricantes devem elaborar a declaração de conformidade UE nos termos do artigo 28.º e apor a marcação CE nos termos do artigo 30.º.

13. Os fabricantes devem manter a documentação técnica e a declaração de conformidade UE à disposição das autoridades de fiscalização do mercado por, pelo menos, 10 anos após a data de colocação no mercado do produto com elementos digitais ou pelo período de apoio, consoante o que for mais longo.

14. Os fabricantes devem assegurar a existência de procedimentos para manter a conformidade com o presente regulamento dos produtos com elementos digitais que façam parte de uma produção em série. Os fabricantes devem 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 a que se refere o artigo 27.º que constituíram a referência para a declaração ou para a verificação da conformidade do produto com elementos digitais.

15. Os fabricantes devem assegurar que os seus produtos com elementos digitais indicam um número de tipo, de lote ou de série, ou outros elementos que permitam a respetiva identificação ou, se tal não for possível, que a informação conste da respetiva embalagem ou de um documento que acompanhe o produto com elementos digitais.

16. Os fabricantes devem indicar o nome, nome comercial registado ou marca registada do fabricante, assim como o endereço postal, o endereço de correio eletrónico ou outros dados de contacto digitais e, se aplicável, o sítio Web no qual o fabricante pode ser contactado no produto com elementos digitais, na respetiva embalagem ou num documento que acompanhe o produto com elementos digitais. Essas informações também devem ser incluídas nas informações e instruções destinadas ao utilizador previstas no anexo II. Os dados de contacto são apresentados numa língua que possa ser facilmente compreendida pelos utilizadores e pelas autoridades de fiscalização do mercado.

17. Para efeitos do presente regulamento, os fabricantes devem designar um ponto de contacto único para permitir que os utilizadores comuniquem direta e rapidamente com eles, nomeadamente para facilitar a comunicação de vulnerabilidades do produto com elementos digitais.

Os fabricantes devem assegurar que o ponto de contacto único seja facilmente identificável pelos utilizadores. Devem também incluir o ponto de contacto único nas informações e instruções destinadas ao utilizador previstas no anexo II.

O ponto de contacto único deve permitir aos utilizadores escolher os seus meios de comunicação preferidos e não deve limitar esses meios a ferramentas automatizadas.

18. Cabe aos fabricantes assegurar que os produtos com elementos digitais são acompanhados das informações e instruções destinadas ao utilizador previstas no anexo II, em papel ou em formato eletrónico. Tais informações e instruções devem ser apresentadas numa língua que possa ser facilmente compreendida pelos utilizadores e pelas autoridades de fiscalização do mercado. Devem ser claras, compreensíveis, inteligíveis e legíveis. Devem permitir a instalação, o funcionamento e a utilização seguros dos produtos com elementos digitais. Os fabricantes devem manter as informações e instruções destinadas ao utilizador previstas no anexo II à disposição dos utilizadores e das autoridades de fiscalização do mercado por, pelo menos, 10 anos após a data de colocação no mercado do produto com elementos digitais ou pelo período de apoio, consoante o que for mais longo. Sempre que essas informações e instruções sejam facultadas em linha, os fabricantes devem assegurar que sejam acessíveis, de fácil utilização e estejam disponíveis por, pelo menos, 10 anos após a data de colocação no mercado do produto com elementos digitais ou pelo período de apoio, consoante o que for mais longo.

19. Os fabricantes devem assegurar que a data final do período de apoio referido no n.º 8 – incluindo, pelo menos, o mês e o ano – é especificada de forma clara e compreensível no momento da compra, de forma facilmente acessível e, se for caso disso, no produto com elementos digitais, na respetiva embalagem ou por meios digitais.

Sempre que seja tecnicamente viável tendo em conta a natureza do produto com elementos digitais, os fabricantes devem apresentar uma notificação aos utilizadores informando-os de que o seu produto com elementos digitais atingiu o fim do respetivo período de apoio.

20. Os fabricantes devem fornecer uma cópia da declaração de conformidade UE ou uma cópia simplificada da declaração de conformidade UE juntamente com o produto com elementos digitais. Caso seja facultada uma declaração de conformidade UE simplificada, esta deve conter o endereço Internet exato onde o texto integral da declaração de conformidade UE pode ser consultado.

21. A partir da colocação no mercado e durante o seu período de apoio, 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 de cibersegurança constantes do anexo I devem tomar imediatamente as medidas corretivas necessárias para assegurar a conformidade do produto com elementos digitais ou dos processos do fabricante, ou para retirar ou recolher esse produto, consoante o caso.

22. Mediante pedido fundamentado de uma autoridade de fiscalização do mercado, os fabricantes devem facultar à referida autoridade, numa língua que possa ser facilmente compreendida por essa autoridade, 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 de cibersegurança 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.

23. Os fabricantes que cessem a sua atividade e, por conseguinte, não estejam em condições de cumprir o disposto 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 pertinentes colocados no mercado, acerca da cessação da atividade iminente por todos os meios disponíveis e tanto quanto possível.

24. A Comissão pode especificar – por meio de atos de execução e tendo em conta as normas europeias e internacionais e as boas práticas – o formato e os elementos da lista de materiais do *software* referidos na parte II, ponto 1, do anexo I. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 62.º, n.º 2.

25. A fim de avaliar a dependência dos Estados-Membros e da União no seu conjunto em relação aos componentes de *software* – e, em especial, aos componentes considerados como *software* livre e de código-fonte aberto –, o ADCO pode decidir realizar uma avaliação, à escala da União, da dependência de categorias específicas de produtos com elementos digitais. Para o efeito, as autoridades de fiscalização do mercado podem solicitar aos fabricantes dessas categorias de produtos com elementos digitais que forneçam as faturas de materiais de *software* pertinentes, tal como referido na parte II, ponto 1, do anexo I. Com base nessas informações, as autoridades de fiscalização do mercado podem prestar ao ADCO informações anonimizadas e agregadas sobre as dependências de *software*. O ADCO apresenta um relatório sobre os resultados da avaliação da dependência ao grupo de cooperação criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555.

Artigo 14.º

Obrigações dos fabricantes em matéria de comunicação de informações

1. Os fabricantes devem notificar qualquer vulnerabilidade ativamente explorada existente no produto com elementos digitais de que tomem conhecimento simultaneamente à CSIRT designada como coordenadora, nos termos do n.º 7 do presente artigo, e à ENISA. Os fabricantes devem notificar essa vulnerabilidade ativamente explorada através da plataforma única de comunicação de informações criada nos termos do artigo 16.º.

2. Para efeitos da notificação referida no n.º 1, o fabricante deve apresentar:

a) Uma notificação de alerta precoce de uma vulnerabilidade ativamente explorada, sem demora injustificada e, em todo o caso, no prazo de 24 horas após o fabricante ter tomado conhecimento da mesma, indicando, se for caso disso, os Estados-Membros em cujo território o fabricante tem conhecimento de que o seu produto com elementos digitais foi disponibilizado;

b) Uma notificação de vulnerabilidade, sem demora injustificada e, em todo o caso, no prazo de 72 horas após o fabricante ter tomado conhecimento da vulnerabilidade ativamente explorada, a menos que as informações pertinentes já tenham sido facultadas, que deve conter informações gerais, conforme disponíveis, sobre o produto com elementos digitais em causa, a natureza geral da exploração e da vulnerabilidade em causa, bem como quaisquer medidas corretivas ou de atenuação tomadas e as medidas corretivas ou de atenuação que os utilizadores podem tomar, e que deve também indicar, se for caso disso, de que forma o fabricante considera sensíveis as informações notificadas;

c) A menos que as informações pertinentes já tenham sido facultadas, o mais tardar, 14 dias após a disponibilização de uma medida corretiva ou de atenuação, um relatório final que inclua, pelo menos, os seguintes elementos:

   i) uma descrição da vulnerabilidade, incluindo a sua gravidade e o seu impacto,

   ii) quando disponíveis, informações relativas a qualquer agente mal-intencionado que tenha explorado ou que esteja a explorar a vulnerabilidade,

   iii) pormenores sobre a atualização de segurança ou outras medidas corretivas que tenham sido disponibilizadas para remediar a vulnerabilidade.

3. Os fabricantes devem notificar qualquer incidente grave que afete a segurança do produto com elementos digitais de que tomem conhecimento simultaneamente à CSIRT designada como coordenadora, nos termos do n.º 7 do presente artigo, e à ENISA. Os fabricantes notificam esse incidente através da plataforma única de comunicação de informações criada nos termos do artigo 16.º.

4. Para efeitos da notificação referida no n.º 3, o fabricante deve apresentar:

a) Uma notificação de alerta precoce de um incidente grave com impacto na segurança do produto com elementos digitais, sem demora injustificada e, em todo o caso, no prazo de 24 horas após o fabricante ter tomado conhecimento do mesmo, incluindo, pelo menos, se há suspeitas de que o incidente foi causado por um ato ilícito ou mal-intencionado e indicando, se for caso disso, os Estados-Membros em cujo território o fabricante tem conhecimento de que o seu produto com elementos digitais foi disponibilizado;

b) Uma notificação de incidente, sem demora injustificada e, em todo o caso, no prazo de 72 horas após o fabricante ter tomado conhecimento do incidente, a menos que as informações pertinentes já tenham sido facultadas, que deve conter informações gerais, se disponíveis, sobre a natureza do incidente, uma avaliação inicial do incidente, bem como quaisquer medidas corretivas ou de atenuação tomadas e medidas corretivas ou de atenuação que os utilizadores podem tomar, e que deve também indicar, se for caso disso, de que forma o fabricante considera sensíveis as informações notificadas;

c) A menos que as informações pertinentes já tenham sido facultadas, no prazo de um mês após a apresentação da notificação de incidente mencionada na alínea b), um relatório final que contenha, no mínimo, os seguintes elementos:

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

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

   iii) medidas de atenuação aplicadas e em curso;

5. Para efeitos do n.º 3, um incidente com impacto na segurança do produto com elementos digitais é considerado grave se:

a) Afeta ou pode afetar negativamente a capacidade de um produto com elementos digitais de proteger a disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou das funções sensíveis ou importantes; ou

b) Provoca ou é capaz de provocar a introdução ou execução de código mal-intencionado num produto com elementos digitais ou nas redes e sistemas de informação de um utilizador do produto com elementos digitais.

6. Se necessário, a CSIRT designada como coordenadora que recebeu inicialmente a notificação pode solicitar aos fabricantes que apresentem um relatório intercalar com informações atualizadas importantes sobre a situação da vulnerabilidade ativamente explorada ou do incidente grave com impacto na segurança do produto com elementos digitais.

7. As notificações a que se referem os n.os 1 e 3 do presente artigo são apresentadas através da plataforma única de comunicação de informações referida no artigo 16.º, utilizando um dos terminais de notificação eletrónica a que se refere o artigo 16.º, n.º 1. A notificação deve ser apresentada utilizando o terminal de notificação eletrónica da CSIRT designada como coordenadora do Estado-Membro em que os fabricantes têm o seu estabelecimento principal na União e deve ser simultaneamente acessível à ENISA.

Para efeitos do presente regulamento, considera-se que um fabricante tem o seu estabelecimento principal na União no Estado-Membro em que são predominantemente tomadas as decisões relacionadas com a cibersegurança dos seus produtos com elementos digitais. Se não for possível determinar esse Estado-Membro, considera-se que o estabelecimento principal se situa no Estado-Membro em que o fabricante em causa tem o estabelecimento com o maior número de trabalhadores na União.

Se um fabricante não tiver um estabelecimento principal na União, deve apresentar as notificações a que se referem os n.os 1 e 3 utilizando o terminal de notificação eletrónica da CSIRT designada como coordenadora no Estado-Membro determinado de acordo com a seguinte ordem e com base nas informações de que o fabricante dispõe:

a) O Estado-Membro em que está estabelecido o mandatário que atua em nome do fabricante para o maior número de produtos com elementos digitais desse fabricante;

b) O Estado-Membro em que está estabelecido o importador que coloca no mercado o maior número de produtos com elementos digitais desse fabricante;

c) O Estado-Membro em que está estabelecido o distribuidor que disponibiliza no mercado o maior número de produtos com elementos digitais desse fabricante;

d) O Estado-Membro em que se situa o maior número de utilizadores de produtos com elementos digitais desse fabricante.

Em relação ao terceiro parágrafo, alínea d), o fabricante pode apresentar notificações relacionadas com qualquer posterior vulnerabilidade ativamente explorada ou incidente grave com impacto na segurança do produto com elementos digitais à mesma CSIRT designada como coordenadora à qual notificou pela primeira vez.

8. Após ter tomado conhecimento de uma vulnerabilidade ativamente explorada ou de um incidente grave com impacto na segurança do produto com elementos digitais, o fabricante deve informar os utilizadores afetados do produto com elementos digitais e, se for caso disso, todos os utilizadores, sobre essa vulnerabilidade ou sobre esse incidente e, se necessário, sobre qualquer medida de atenuação dos riscos e quaisquer medidas corretivas que os utilizadores possam tomar para atenuar o impacto dessa vulnerabilidade ou incidente, se for caso disso, num formato estruturado e legível por máquina que seja facilmente processável automaticamente. Caso o fabricante não informe atempadamente os utilizadores do produto com elementos digitais, as CSIRT designadas como coordenadoras notificadas podem prestar essas informações aos utilizadores quando consideradas proporcionais e necessárias para prevenir ou atenuar o impacto dessa vulnerabilidade ou incidente.

9. Até 11 de dezembro de 2025, a Comissão adota atos delegados nos termos do artigo 61.º do presente regulamento, a fim de completar o presente regulamento especificando os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações a que se refere o artigo 16.º, n.º 2, do presente regulamento. A Comissão coopera com a rede das CSIRT criada nos termos do artigo 15.º da Diretiva (UE) 2022/2555 e com a ENISA na elaboração dos projetos de atos delegados.

10. A Comissão pode especificar mais aprofundadamente, por meio de atos de execução, o formato e os procedimentos das notificações a que se refere o presente artigo e os artigos 15.º e 16.º. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 62.º, n.º 2. A Comissão coopera com a rede das CSIRT e a ENISA na elaboração desses projetos de atos de execução.

Artigo 15.º

Transmissão voluntária de informações

1. Os fabricantes e outras pessoas singulares ou coletivas podem notificar voluntariamente a uma CSIRT designada como coordenadora ou à ENISA qualquer vulnerabilidade contida num produto com elementos digitais, bem como ciberameaças que possam afetar o perfil de risco de um produto com elementos digitais.

2. Os fabricantes e outras pessoas singulares ou coletivas podem notificar voluntariamente a uma CSIRT designada como coordenadora ou à ENISA qualquer incidente com impacto na segurança do produto com elementos digitais, bem como quase incidentes que pudessem ter resultado num incidente desse tipo.

3. A CSIRT designada coordenadora ou a ENISA deve tratar as notificações a que se referem os n.os 1 e 2 do presente artigo de acordo com o procedimento previsto no artigo 16.º.

A CSIRT designada coordenadora pode dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias.

4. Caso uma pessoa singular ou coletiva que não o fabricante notifique uma vulnerabilidade ativamente explorada ou um incidente grave com impacto na segurança de um produto com elementos digitais em conformidade com os n.os 1 ou 2, a CSIRT designada como coordenadora deve informar o fabricante sem demora injustificada.

5. A CSIRT designada como coordenadora e a ENISA devem garantir a confidencialidade e a proteção adequada das informações facultadas pela pessoa singular ou coletiva notificadora. Sem prejuízo da prevenção, investigação, deteção e repressão de infrações penais, a notificação voluntária não pode dar origem à imposição de quaisquer obrigações adicionais a uma pessoa singular ou coletiva notificadora, às quais esta não estaria sujeita se não tivesse apresentado a notificação.

Artigo 16.º

Criação de uma plataforma única de comunicação de informações

1. Para efeitos das notificações referidas no artigo 14.º, n.os 1 e 3, e no artigo 15.º, n.os 1 e 2, e a fim de simplificar as obrigações dos fabricantes em matéria de comunicação de informações, a ENISA deve criar uma plataforma única de comunicação de informações. As operações quotidianas dessa plataforma única de comunicação de informações devem ser geridas e mantidas pela ENISA. A arquitetura da plataforma única de comunicação de informações deve permitir que os Estados-Membros e a ENISA apliquem os seus próprios terminais de notificação eletrónica.

2. Após receber uma notificação, a CSIRT designada como coordenadora que inicialmente recebeu a notificação deve divulgar, sem demora, a notificação através da plataforma única de comunicação de informações às CSIRT designadas como coordenadoras em cujo território o fabricante tenha indicado que o produto com elementos digitais foi disponibilizado.

Em circunstâncias excecionais e especialmente a pedido do fabricante e tendo em conta o grau de sensibilidade das informações notificadas – tal como indicado pelo fabricante nos termos do artigo 14.º, n.º 2, alínea a), do presente regulamento –, a divulgação da notificação pode ser adiada com base em motivos fundamentados relacionados com a cibersegurança durante um período de tempo estritamente necessário, incluindo nos casos em que uma vulnerabilidade esteja sujeita a um procedimento de divulgação coordenada de vulnerabilidades a que se refere o artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555. Caso uma CSIRT decida reter uma notificação, deve informar imediatamente a ENISA da decisão e apresentar uma justificação para a mesma, bem como indicar quando irá divulgar a notificação em conformidade com o procedimento de divulgação previsto no presente número. A ENISA pode apoiar a CSIRT na invocação de motivos relacionados com a cibersegurança para o adiamento da divulgação da notificação.

Em circunstâncias particularmente excecionais, se na notificação referida no artigo 14.º, n.º 2, alínea b), o fabricante indicar:

a) Que a vulnerabilidade notificada foi ativamente explorada por um agente mal-intencionado e que, de acordo com as informações disponíveis, não foi explorada em nenhum outro Estado-Membro além do da CSIRT designada como coordenadora à qual o fabricante notificou a vulnerabilidade;

b) Que qualquer nova divulgação imediata da vulnerabilidade notificada é suscetível de resultar na prestação de informações cuja divulgação seria contrária aos interesses essenciais desse Estado-Membro; ou

c) Que a vulnerabilidade notificada representa um elevado risco iminente de cibersegurança decorrente de uma maior divulgação;

apenas são disponibilizadas simultaneamente à ENISA a informação de que o fabricante efetuou uma notificação, informações gerais sobre o produto, a informação sobre a natureza geral da exploração e a informação de que foram invocados motivos relacionados com a segurança, até que a notificação completa seja divulgada às CSIRT em causa e à ENISA. Se a ENISA, com base nessas informações, considerar que existe um risco sistémico que afeta a segurança no mercado interno, ela recomenda à CSIRT destinatária que divulgue a notificação completa às outras CSIRT designadas como coordenadoras e à própria ENISA.

3. Após receberem uma notificação de uma vulnerabilidade ativamente explorada num produto com elementos digitais ou de um incidente grave com impacto na segurança de um produto com elementos digitais, as CSIRT designadas como coordenadoras devem facultar às autoridades de fiscalização do mercado dos respetivos Estados-Membros as informações notificadas necessárias para que essas autoridades cumpram as suas obrigações nos termos do presente regulamento.

4. A ENISA deve tomar medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança da plataforma única de comunicação de informações e das informações apresentadas ou divulgadas através dessa plataforma. Ela notifica à rede das CSIRT e à Comissão, sem demora injustificada, qualquer incidente de segurança que afete a plataforma única de comunicação de informações.

5. A ENISA, em cooperação com a rede das CSIRT, deve fornecer e aplicar especificações sobre as medidas técnicas, operacionais e organizativas relativas à criação, manutenção e funcionamento seguro da plataforma única de comunicação de informações a que se refere o n.º 1, incluindo, pelo menos, as disposições de segurança relacionadas com a criação, funcionamento e manutenção da plataforma única de comunicação de informações, bem como os terminais de notificação eletrónica criados pelas CSIRT designadas como coordenadoras a nível nacional e a ENISA a nível da União, incluindo os aspetos processuais para assegurar que nos casos em que uma vulnerabilidade notificada não tenha medidas corretivas ou de atenuação disponíveis, as informações sobre essa vulnerabilidade são partilhadas em conformidade com protocolos de segurança rigorosos e com base na «necessidade de conhecer».

6. Caso uma CSIRT designada como coordenadora tenha tomado conhecimento de uma vulnerabilidade ativamente explorada no âmbito de um procedimento de divulgação coordenada de vulnerabilidades a que se refere o artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555, a CSIRT designada como coordenadora que inicialmente recebeu a notificação pode atrasar a divulgação da notificação pertinente através da plataforma única de comunicação de informações com base em motivos fundamentados relacionados com a cibersegurança durante um período que não exceda o estritamente necessário e até ser dado o consentimento das partes envolvidas na divulgação coordenada de vulnerabilidades. Esse requisito não impede os fabricantes de notificarem voluntariamente essa vulnerabilidade, em conformidade com o procedimento previsto no presente artigo.

Artigo 17.º

Outras disposições relacionadas com a comunicação

1. A ENISA pode apresentar à Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe), criada nos termos do artigo 16.º da Diretiva (UE) 2022/2555, informações notificadas nos termos do artigo 14.º, n.ºs 1 e 3, e do artigo 15.º, n.ºs 1 e 2, do presente regulamento se tais informações forem relevantes para a gestão coordenada de incidentes e crises de cibersegurança em grande escala a um nível operacional. Para efeitos de determinação dessa relevância, a ENISA pode considerar análises técnicas realizadas pela rede das CSIRT, se disponíveis.

2. Nos casos em que seja necessário sensibilizar o público para evitar ou atenuar um incidente grave com impacto na segurança do produto com elementos digitais ou para lidar com um incidente em curso, ou se a divulgação do incidente for de interesse público, a CSIRT designada como coordenadora do Estado-Membro em causa pode – após consultar o fabricante em causa e, se for caso disso, em cooperação com a ENISA – informar o público sobre o incidente ou exigir que o fabricante o faça.

3. Com base nas notificações recebidas nos termos do artigo 14.º, n.ºs 1 e 3, e do artigo 15.º, n.ºs 1 e 2, do presente regulamento a ENISA elabora, de 24 em 24 meses, 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 criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555. O primeiro desses relatórios deve ser apresentado no prazo de 24 meses a contar da data de aplicação das obrigações previstas no artigo 14.º, n.ºs 1 e 3. A ENISA deve incluir as informações relevantes dos seus relatórios técnicos no seu relatório sobre o estado da cibersegurança na União, nos termos do artigo 18.º da Diretiva (UE) 2022/2555.

4. O simples ato de notificação nos termos do artigo 14.º, n.ºs 1 e 3, ou do artigo 15.º, n.ºs 1 e 2, não sujeita a pessoa singular ou coletiva notificante a uma responsabilidade acrescida.

5. Após a disponibilização de uma atualização de segurança ou de outro tipo de medidas corretivas ou de atenuação, a ENISA – com o acordo do fabricante do produto com elementos digitais em causa – acrescentará a vulnerabilidade conhecida publicamente e notificada nos termos do artigo 14.º, n.º 1, ou do artigo 15.º, n.º 1, do presente regulamento à base de dados europeia de vulnerabilidades criada nos termos do artigo 12.º, n.º 2, da Diretiva (UE) 2022/2555.

6. As CSIRT designadas como coordenadoras prestam serviço de assistência aos fabricantes relativamente às obrigações de comunicação de informações previstas no artigo 14.º,– e em especial aos fabricantes que sejam considerados microempresas ou pequenas ou médias empresas.

Artigo 18.º

Mandatários

1. Os fabricantes podem designar um mandatário por meio de um mandato escrito.

2. Não fazem parte do mandato do mandatário as obrigações previstas no artigo 13.º, n.ºs 1 a 11, no artigo 13.º, n.º 12, primeiro parágrafo, e no artigo 13.º, n.º 14.

3. O mandatário pratica os atos especificados no mandato conferido pelo fabricante. O mandatário deve facultar uma cópia do mandato às autoridades de fiscalização do mercado, mediante pedido. 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 28.º e a documentação técnica referida no artigo 31.º durante, pelo menos, 10 anos após a data de colocação do produto com elementos digitais no mercado ou durante o período de apoio, consoante o que for mais longo;

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 19.º

Obrigações dos importadores

1. Os importadores podem colocar no mercado apenas produtos com elementos digitais que cumpram os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e se os processos aplicados pelo fabricante cumprirem os requisitos essenciais de cibersegurança constantes da parte II do anexo I.

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 32.º;

b) O fabricante elaborou a documentação técnica;

c) O produto com elementos digitais ostenta a marcação CE referida no artigo 30.º e é acompanhado da declaração de conformidade UE referida no artigo 13.º, n.º 20, e das informações e instruções de utilização previstas no anexo II numa língua que possa ser facilmente compreendida pelos utilizadores e pelas autoridades de fiscalização do mercado;

d) O fabricante respeitou os requisitos previstos no artigo 13.º, n.ºs 15, 16 e 19.

Para efeitos do presente número, os importadores devem poder apresentar os documentos necessários que comprovem o cumprimento dos requisitos estabelecidos no presente artigo.

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 o presente regulamento, o importador não pode colocar o produto no mercado antes de se assegurar a conformidade desse produto ou dos processos aplicados pelo fabricante com o presente regulamento. 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.

Sempre que um importador tenha motivos para crer que um produto com elementos digitais pode apresentar um risco de cibersegurança significativo à luz de fatores de risco não técnicos, o importador deve informar desse facto as autoridades de fiscalização do mercado. Após a receção dessas informações, as autoridades de fiscalização do mercado devem seguir os procedimentos referidos no artigo 54.º, n.º 2.

4. Os importadores devem indicar o seu nome, nome comercial registado ou marca registada, o endereço postal, o endereço de correio eletrónico ou outros dados de contacto digitais e, se disponível, o sítio Web de contacto no produto com elementos digitais ou 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 distribuidores que saibam ou tenham motivos para crer que um produto com elementos digitais que colocaram no mercado não está em conformidade com o presente regulamento devem tomar imediatamente as medidas corretivas necessárias para assegurar a conformidade do produto em causa com o presente regulamento, ou para retirar ou recolher o produto, se for caso disso.

Ao tomarem conhecimento de 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.

6. Durante o prazo de, pelo menos, 10 anos após a data de colocação no mercado do produto com elementos digitais ou durante o período de apoio, consoante o que for mais longo, 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.

7. 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 de cibersegurança constantes da parte I do anexo I, bem como a conformidade dos processos aplicados pelo fabricante com os requisitos essenciais de cibersegurança constantes da parte II 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 colocado no mercado.

8. Se 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 20.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 definidos no 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 13.º, n.ºs 15, 16, 18, 19 e 20, e no artigo 19.º, n.º 4, e facultaram todos os documentos necessários ao distribuidor.

3. Sempre que, com base nas informações de que dispõe, 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 de cibersegurança constantes do anexo I, o distribuidor não pode disponibilizar o produto em causa no mercado antes de o produto ou de os processos aplicados pelo fabricante estarem em conformidade com o presente regulamento. 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 sem demora injustificada.

4. Os distribuidores que saibam ou, com base nas informações de que dispõem, 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 o presente regulamento 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 para retirar ou recolher o produto, se for caso disso.

Ao tomarem conhecimento de 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, facultando-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 o presente regulamento. 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, com base nas informações de que dispõe, deve informar desse facto, sem demora injustificada, 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 21.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 ao disposto nos artigos 13.º e 14.º, 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 22.º

Outros casos em que se aplicam as obrigações dos fabricantes

1. Para efeitos do presente regulamento, a pessoa singular ou coletiva, distinta do fabricante, do importador ou do distribuidor, que proceda a uma modificação substancial de um produto com elementos digitais e que disponibilize esse produto no mercado é considerada um fabricante.

2. A pessoa a que se refere o n.º 1 do presente artigo fica sujeita às obrigações estabelecidas nos artigos 13.º e 14.º relativamente à parte do produto com elementos digitais 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 23.º

Identificação dos operadores económicos

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

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

b) Sempre que disponíveis, 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 10 anos após lhes ter sido fornecido o produto com elementos digitais e de 10 anos após terem fornecido o produto com elementos digitais.

Artigo 24.º

Obrigações dos administradores de* software *de código-fonte aberto

1. Os administradores de *software* de código-fonte aberto devem pôr em prática e documentar, de uma forma verificável, uma política de cibersegurança para promover o desenvolvimento de um produto com elementos digitais seguro, bem como um tratamento eficaz das vulnerabilidades pelos criadores desse produto. Essa política também deve promover a comunicação voluntária de vulnerabilidades pelos criadores desse produto, tal como previsto no artigo 15.º, e ter em conta a natureza específica do administrador de *software* de código-fonte aberto e as disposições jurídicas e organizativas a que está sujeito. Essa política deve incluir, em especial, aspetos relacionados com a documentação, o tratamento e a correção de vulnerabilidades e promover a partilha de informações sobre vulnerabilidades detetadas pela comunidade de código-fonte aberto.

2. Os administradores de *software* de código-fonte aberto devem cooperar com as autoridades de fiscalização do mercado, a pedido destas, com vista a atenuar os riscos de cibersegurança colocados por um produto com elementos digitais que seja considerado *software* livre e de código-fonte aberto.

Na sequência de um pedido fundamentado de uma autoridade de fiscalização do mercado, os administradores de *software* de código-fonte aberto devem facultar a essa autoridade – numa língua que possa ser facilmente compreendida por essa autoridade – a documentação referida no n.º 1, em papel ou em suporte eletrónico.

3. As obrigações estabelecidas no artigo 14.º, n.º 1, aplicam-se aos administradores de *software* de código-fonte aberto, na medida em que estejam envolvidos no desenvolvimento de produtos com elementos digitais. As obrigações estabelecidas no artigo 14.º, n.ºs 3 e 8, aplicam-se aos administradores de *software* de código-fonte aberto, na medida em que incidentes graves com impacto na segurança dos produtos com elementos digitais afetem as redes e os sistemas de informação fornecidos pelos administradores de *software* de código-fonte aberto para o desenvolvimento desses produtos.

Artigo 25.º

Certificado de segurança do* software *livre e de código-fonte aberto

Com vista a facilitar o cumprimento da obrigação de exercer a diligência devida, estabelecida no artigo 13.º, n.º 5, em particular no que diz respeito aos fabricantes que integram componentes de *software* livre e de código-fonte aberto nos seus produtos com elementos digitais, a Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 61.º para completar o presente regulamento estabelecendo programas voluntários de certificação de segurança que permitam aos programadores ou aos utilizadores de produtos com elementos digitais que sejam considerados *software* livre e de código-fonte aberto, bem como a terceiros, avaliar a conformidade desses produtos com a totalidade ou parte dos requisitos essenciais de cibersegurança ou de outras obrigações estabelecidos no presente regulamento.

Artigo 26.º

Orientações

1. A fim de simplificar a aplicação e garantir a respetiva coerência, a Comissão publica orientações para ajudar os operadores económicos a aplicar o presente regulamento, dando especial destaque à facilitação do cumprimento por parte das microempresas e das pequenas e médias empresas.

2. Sempre que pretenda emitir orientações nos termos do n.º 1, a Comissão deve ter em conta, pelo menos, os seguintes aspetos:

a) O âmbito de aplicação do presente regulamento, com especial ênfase em soluções de tratamento remoto de dados e de *software* livre e de código-fonte aberto;

b) A aplicação de períodos de apoio em relação a categorias específicas de produtos com elementos digitais;

c) Orientações dirigidas aos fabricantes abrangidos pelo presente regulamento que estejam também sujeitos a legislação de harmonização da União distinta do presente regulamento ou a outros atos jurídicos conexos da União;

d) O conceito de modificação substancial.

A Comissão deve igualmente manter uma lista de fácil acesso que indique os atos delegados e de execução adotados nos termos do presente regulamento.

3. Ao elaborar as orientações nos termos do presente artigo, a Comissão deve consultar as partes interessadas pertinentes.

CAPÍTULO III

CONFORMIDADE DO PRODUTO COM ELEMENTOS DIGITAIS

Artigo 27.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 de cibersegurança estabelecidos no anexo I, abrangidos pelas referidas normas ou partes destas.

A Comissão, em conformidade com o artigo 10.º, n.º 1, do Regulamento (UE) n.º 1025/2012, deve solicitar a uma ou várias organizações europeias de normalização que elaborem normas harmonizadas para os requisitos essenciais de cibersegurança previstos no anexo I do presente regulamento. Ao elaborar pedidos de normalização para o presente regulamento, a Comissão deve procurar ter em conta as normas europeias e internacionais existentes em matéria de cibersegurança que estejam em vigor ou em fase de desenvolvimento, a fim de simplificar a conceção de normas harmonizadas, em conformidade com o Regulamento (UE) n.º 1025/2012.

2. A Comissão fica habilitada a adotar atos de execução para estabelecer especificações comuns abrangendo requisitos técnicos que prevejam meios para cumprir os requisitos essenciais de cibersegurança previstos no anexo I para os produtos com elementos digitais abrangidos pelo âmbito de aplicação do presente regulamento.

Os referidos atos de execução só são adotados se estiverem preenchidas as seguintes condições:

a) A Comissão solicitou, nos termos do artigo 10.º, n.º 1, do Regulamento (UE) n.º 1025/2012, a uma ou várias organizações europeias de normalização a elaboração de normas harmonizadas relativas aos requisitos essenciais de cibersegurança estabelecidos no anexo I, e:

   i) o pedido não foi aceite,

   ii) as normas harmonizadas que dão resposta a esse pedido não foram elaboradas dentro do prazo fixado nos termos do artigo 10.º, n.º 1, do Regulamento (UE) n.º 1025/2012, ou

   iii) as normas harmonizadas não estão em conformidade com o pedido; e

b) Não se encontra publicada no *Jornal Oficial da União Europeia* qualquer referência a normas harmonizadas que abranjam os requisitos essenciais de cibersegurança pertinentes previstos no anexo I do presente regulamento, em conformidade com o Regulamento (UE) n.º 1025/2012, e não se prevê a publicação de tal referência dentro de um prazo razoável.

Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 62.º, n.º 2.

3. Antes de elaborar o projeto de ato de execução referido no n.º 2 do presente artigo, a Comissão informa o comité a que se refere o artigo 22.º do Regulamento (UE) n.º 1025/2012 de que considera que estão preenchidas as condições previstas no n.º 2 do presente artigo.

4. Na elaboração do projeto de ato de execução referido no n.º 2, a Comissão toma em consideração os pareceres de organismos pertinentes e consulta, nos devidos termos, todas as partes interessadas pertinentes.

5. Presume-se que os produtos com elementos digitais e os processos aplicados pelo fabricante que estão em conformidade com as especificações comuns estabelecidas pelos atos de execução a que se refere o n.º 2 do presente artigo, ou com partes dessas especificações comuns, estão conformes com os requisitos essenciais de cibersegurança constantes do anexo I, abrangidos por tais especificações comuns ou por partes delas.

6. Quando uma norma harmonizada é adotada por uma organização de normalização europeia e proposta à Comissão para publicação da sua referência no *Jornal Oficial da União Europeia*, a Comissão avalia a norma harmonizada em conformidade com o Regulamento (UE) n.º 1025/2012. Quando a referência de uma norma harmonizada é publicada no *Jornal Oficial da União Europeia*, a Comissão revoga os atos de execução mencionados no n.º 2 do presente artigo, ou partes destes, que abranjam os mesmos requisitos essenciais de cibersegurança que são abrangidos por essa norma harmonizada.

7. Quando um Estado-Membro considera que uma especificação comum não satisfaz totalmente os requisitos essenciais de cibersegurança estabelecidos no anexo I, informa a Comissão desse facto apresentando uma explicação pormenorizada. A Comissão avalia essa explicação pormenorizada e pode, se for caso disso, alterar o ato de execução que estabelece a especificação comum em causa.

8. 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 estão conformes com os requisitos essenciais de cibersegurança estabelecidos no anexo I, desde que a declaração de conformidade UE ou o certificado europeu de cibersegurança, ou partes destes, abranjam esses requisitos.

9. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º do presente regulamento para o completar especificando os sistemas europeus de certificação da cibersegurança adotados nos termos do Regulamento (UE) 2019/881 que podem ser utilizados para demonstrar a conformidade dos produtos com elementos digitais com os requisitos essenciais de cibersegurança estabelecidos no anexo I, ou partes destes. Além disso, a emissão de um certificado europeu de cibersegurança ao abrigo dos referidos sistemas, cujo nível de garantia corresponda, no mínimo, a «substancial», elimina a obrigação que incumbe ao fabricante de realizar uma avaliação da conformidade por terceiros para os requisitos correspondentes, tal como estabelecido no artigo 32.º, n.º 2, alíneas a) e b), e n.º 3, alíneas a) e b), do presente regulamento.

Artigo 28.º

Declaração de conformidade UE

1. A declaração de conformidade UE é elaborada pelos fabricantes nos termos do artigo 13.º, n.º 12, e indica que o cumprimento dos requisitos essenciais de cibersegurança aplicáveis constantes do anexo I foi demonstrado.

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

A declaração de conformidade UE simplificada a que se refere o artigo 13.º, n.º 20, respeita o modelo que consta do anexo VI. Deve ser disponibilizada nas 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 jurídico da União que exija uma declaração de conformidade UE, deve ser elaborada uma declaração de conformidade UE única referente a todos esses atos jurídicos da União. Essa declaração deve conter a identificação dos atos jurídicos 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 com elementos digitais.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 61.º para completar o presente regulamento acrescentando elementos ao conteúdo mínimo da declaração de conformidade UE constante do anexo V, de forma a ter em conta a evolução tecnológica.

Artigo 29.º

Princípios gerais da marcação CE

A marcação CE está sujeita aos princípios gerais enunciados no artigo 30.º do Regulamento (CE) n.º 765/2008.

Artigo 30.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 28.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 28.º ou no sítio Web que acompanha o produto de *software*. Neste último caso, a secção pertinente do sítio Web deve ser de acesso fácil e direto para os consumidores.

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 em matéria de cibersegurança 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 32.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 de harmonização da União distinta do presente regulamento que também preveja a aposição da marcação CE, a marcação deve indicar que o produto cumpre igualmente os requisitos definidos nessa outra legislação de harmonização da União.

6. A Comissão pode estabelecer, por meio de atos de execução, especificações técnicas para os rótulos, pictogramas ou quaisquer outras marcas relacionadas com a segurança dos produtos com elementos digitais, bem como os seus períodos de apoio e mecanismos para promover a sua utilização e aumentar a sensibilização do público para a segurança dos produtos com elementos digitais. Ao elaborar os projetos de atos de execução, a Comissão consulta as partes interessadas pertinentes e, se já tiver sido criado nos termos do artigo 52.º, n.º 15, o ADCO. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 62.º, n.º 2.

Artigo 31.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 de cibersegurança estabelecidos no anexo I. Deve conter, no mínimo, os elementos constantes do anexo VII.

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 período de apoio, no mínimo.

3. No caso dos produtos com elementos digitais a que se refere o artigo 12.º que também sejam abrangidos por outros atos jurídicos da União que prevejam a disponibilização de documentação técnica, deve elaborar-se uma documentação técnica única que contenha as informações referidas no anexo VII do presente regulamento e as informações exigidas por esses atos jurídicos 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 61.º para completar o presente regulamento acrescentando elementos a incluir na documentação técnica constante do anexo VII, de modo a ter em conta a evolução tecnológica, bem como a evolução verificada no processo de execução do presente regulamento. Para o efeito, a Comissão faz os possíveis para assegurar que os encargos administrativos para as microempresas e para as pequenas e médias empresas são proporcionados.

Artigo 32.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 de cibersegurança constantes do anexo I. Cabe ao fabricante demonstrar a conformidade com os requisitos essenciais de cibersegurança recorrendo a qualquer dos seguintes procedimentos:

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

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

c) Uma avaliação da conformidade baseada na garantia de qualidade total (com base no módulo H) prevista no anexo VIII; ou

d) Se disponível e aplicável, um sistema europeu de certificação da cibersegurança, nos termos do artigo 27.º, n.º 9.

2. Sempre que, ao avaliar a conformidade de um produto importante com elementos digitais pertencente à classe I, conforme estabelecido no anexo III, e dos processos aplicados pelo seu fabricante com os requisitos essenciais de cibersegurança constantes do anexo I, o fabricante não tiver aplicado ou tiver aplicado apenas parcialmente normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança cujo nível de garantia corresponda, no mínimo, a «substancial» referidos no artigo 27.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 cibersegurança, de qualquer dos seguintes procedimentos:

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

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

3. Sempre que o produto for um produto importante com elementos digitais pertencente à classe II, previsto no anexo III, o fabricante deve demonstrar a conformidade com os requisitos essenciais de cibersegurança constantes do anexo I recorrendo a qualquer dos seguintes procedimentos:

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

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

c) Se disponível e aplicável, um sistema europeu de certificação da cibersegurança nos termos do artigo 27.º, n.º 9, do presente regulamento cujo nível de garantia corresponda, no mínimo, a «substancial» em conformidade com o Regulamento (UE) 2019/881.

4. A conformidade dos produtos críticos com elementos digitais enumerados no anexo IV com os requisitos essenciais de cibersegurança constantes do anexo I deve ser demonstrada recorrendo a um dos seguintes procedimentos:

a) Um sistema europeu de certificação da cibersegurança, em conformidade com o artigo 8.º, n.º 1; ou

b) Se as condições previstas no artigo 8.º, n.º 1, não estiverem preenchidas, qualquer dos procedimentos a que se refere o n.º 3 do presente artigo.

5. Os fabricantes de produtos com elementos digitais que sejam considerados *software* livre e de código-fonte aberto, abrangidos pelas categorias definidas no anexo III, devem poder demonstrar a conformidade com os requisitos essenciais de cibersegurança constantes do anexo I recorrendo a um dos procedimentos referidos no n.º 1 do presente artigo, desde que a documentação técnica a que se refere o artigo 31.º seja disponibilizada ao público no momento da colocação desses produtos no mercado.

6. Os interesses e necessidades específicos das microempresas e das pequenas e médias empresas, incluindo as empresas em fase de arranque, devem ser tidos em conta aquando da fixação das taxas aplicáveis aos procedimentos de avaliação da conformidade, devendo essas taxas ser reduzidas de forma proporcional aos referidos interesses e necessidades específicos.

Artigo 33.º

Medidas de apoio para as microempresas e as pequenas e médias empresas, incluindo as empresas em fase de arranque

1. Os Estados-Membros devem, se adequado, empreender as seguintes ações, adaptadas às necessidades das microempresas e das pequenas empresas:

a) Organizar atividades específicas de sensibilização e formação sobre a aplicação do presente regulamento;

b) Criar um canal específico para a comunicação com as microempresas e as pequenas empresas e, se for caso disso, com as autoridades públicas locais, a fim de prestar aconselhamento e responder a perguntas sobre a aplicação do presente regulamento;

c) Apoiar as atividades de ensaio e de avaliação da conformidade, nomeadamente, se for caso disso, com o apoio do Centro Europeu de Competências em Cibersegurança.

2. Os Estados-Membros podem, se adequado, criar ambientes de teste da regulamentação em matéria de ciber-resiliência. Tais ambientes de teste da regulamentação devem estabelecer ambientes de ensaio controlados para produtos inovadores com elementos digitais, a fim de facilitar o seu desenvolvimento, conceção, validação e ensaio para efeitos do cumprimento do presente regulamento durante um período limitado antes da colocação no mercado. A Comissão e, se adequado, a ENISA podem oferecer apoio técnico, aconselhamento e instrumentos para a criação e o funcionamento de ambientes de teste da regulamentação. Os ambientes de teste da regulamentação são criados sob a supervisão, a orientação e o apoio diretos das autoridades de fiscalização do mercado. Os Estados-Membros informam a Comissão e as demais autoridades de fiscalização do mercado da criação de um ambiente de teste da regulamentação através do ADCO. Os ambientes de teste da regulamentação não afetam os poderes de supervisão e de correção das autoridades competentes. Os Estados-Membros devem assegurar um acesso aberto, justo e transparente aos ambientes de teste da regulamentação e, em particular, facilitar o acesso das microempresas e das pequenas empresas, incluindo as empresas em fase de arranque.

3. Nos termos do artigo 26.º, a Comissão fornece orientações às microempresas e às pequenas e médias empresas no que respeita à aplicação do presente regulamento.

4. A Comissão divulga o apoio financeiro disponível no âmbito do regime regulamentar dos programas da União existentes, em especial com vista a aliviar os encargos financeiros das microempresas e das pequenas empresas.

5. As microempresas e as pequenas empresas podem facultar todos os elementos da documentação técnica especificada no anexo VII utilizando um formato simplificado. Para o efeito, a Comissão especifica, por meio de atos de execução, o formulário simplificado de documentação técnica tendo em conta as necessidades das microempresas e das pequenas empresas, incluindo a forma como os elementos previstos no anexo VII devem ser facultados. Sempre que uma microempresa ou pequena empresa opte por prestar as informações previstas no anexo VII de forma simplificada, deve utilizar o formulário referido no presente número. Os organismos notificados aceitam esse formulário para efeitos da avaliação da conformidade.

Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 62.º, n.º 2.

Artigo 34.º

Acordos de reconhecimento mútuo

Tendo em conta o nível de desenvolvimento técnico e a abordagem em matéria de avaliação da conformidade de um país terceiro, a União pode celebrar acordos de reconhecimento mútuo com países terceiros, nos termos do artigo 218.º do TFUE, com o objetivo de promover e facilitar o comércio internacional.

CAPÍTULO IV

NOTIFICAÇÃO DOS ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Artigo 35.º

Notificação

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

2. Os Estados-Membros devem fazer os possíveis para garantir, até 11 de dezembro de 2026, a existência de um número suficiente de organismos notificados na União para a realização de avaliações da conformidade, de molde a evitar estrangulamentos e obstáculos à entrada no mercado.

Artigo 36.º

Autoridades notificadoras

1. Cada Estados-Membro deve designar uma autoridade notificadora responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação de organismos de avaliação da conformidade e pelo controlo dos mesmos, inclusive no que respeita ao cumprimento do artigo 41.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.

3. Se a autoridade notificadora delegar ou, a outro título, atribuir as tarefas de avaliação, notificação ou controlo a que se refere o n.º 1 a um organismo que não seja público, esse organismo deve ser uma pessoa coletiva e cumprir, com as devidas adaptações, o disposto no artigo 37.º. Além disso, esse organismo deve dotar-se de capacidade para garantir a cobertura da responsabilidade civil decorrente das atividades que exerce.

4. A autoridade notificadora deve assumir a plena responsabilidade pelas tarefas executadas pelo organismo a que se refere o n.º 3.

Artigo 37.º

Requisitos relativos às autoridades notificadoras

1. As autoridades notificadoras devem ser constituídas de modo a evitar conflitos de interesses 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 38.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 ao público as informações a que se refere o n.º 1.

Artigo 39.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 com elementos digitais que avaliam.

Pode considerar-se como organismo terceiro 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 interesses.

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 importador, o distribuidor, 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 importação, na distribuição, na comercialização, na instalação, na utilização ou na manutenção desses produtos com elementos digitais que avaliam, 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 subcontratados 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 VIII 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.

Os organismos de avaliação da conformidade devem dispor dos meios necessários para a boa execução das tarefas técnicas e administrativas relacionadas com as atividades de avaliação da conformidade e devem ter acesso a todos os equipamentos e 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 de cibersegurança previstos no anexo I, das normas harmonizadas aplicáveis e das especificações comuns, bem como das disposições aplicáveis da legislação de harmonização da União e dos atos de 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 seu Estado-Membro 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 VIII 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 51.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, proporcionadas e razoáveis, evitando criar encargos desnecessários para os operadores económicos e tendo particularmente em conta os interesses das microempresas e das pequenas e médias empresas no que respeita às taxas.

Artigo 40.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 39.º, na medida em que as normas harmonizadas aplicáveis abranjam esses requisitos.

Artigo 41.º

Filiais e subcontratados 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 subcontratado ou a filial cumpre os requisitos previstos no artigo 39.º e informar a autoridade notificadora desse facto.

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

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

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

Artigo 42.º

Pedido de notificação

1. Os organismos de avaliação da conformidade devem apresentar um pedido de 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 dos procedimentos de avaliação da conformidade e do produto ou dos produtos com elementos digitais em relação aos quais os organismos se consideram competentes, bem como, se aplicável, de um certificado de acreditação emitido por um organismo nacional de acreditação, atestando que os organismos de avaliação da conformidade cumprem os requisitos estabelecidos no artigo 39.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 39.º.

Artigo 43.º

Procedimento de notificação

1. As autoridades notificadoras devem notificar apenas os organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 39.º.

2. A autoridade notificadora deve notificar a Comissão e os demais Estados-Membros por meio do sistema de informação «Nova abordagem em matéria de organismos notificados e designados», desenvolvido e gerido pela Comissão.

3. A notificação deve incluir dados completos das atividades de avaliação da conformidade, do módulo ou módulos de avaliação da conformidade e do produto ou produtos com elementos digitais em causa, bem como a certificação de competência pertinente.

4. Se a notificação não se basear no certificado de acreditação referido no artigo 42.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 39.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 44.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 jurídicos 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 45.º

Alterações das notificações

1. Sempre que determinar ou for informada de que um organismo notificado deixou de cumprir os requisitos previstos no artigo 39.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 46.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 47.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 32.º e no anexo VIII.

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, designadamente no que respeita às microempresas e às pequenas e médias empresas, a dimensão, o setor e a estrutura das empresas, o grau de complexidade e o nível de risco de cibersegurança dos produtos com elementos digitais e da tecnologia 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 a conformidade dos produtos com elementos digitais com o presente regulamento.

4. Se verificar que um fabricante não cumpriu os requisitos estabelecidos no anexo I, nas normas harmonizadas correspondentes ou nas especificações comuns referidas no artigo 27.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 com elementos digitais 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 48.º

Recurso das decisões dos organismos notificados

Os Estados-Membros asseguram a existência de procedimentos de recurso das decisões dos organismos notificados.

Artigo 49.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 com elementos digitais, as informações relevantes sobre questões relativas aos resultados negativos da avaliação da conformidade e, mediante pedido, sobre questões relativas aos resultados positivos da mesma.

Artigo 50.º

Intercâmbio de experiências

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

Artigo 51.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 52.º

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

1. O Regulamento (UE) 2019/1020 é aplicável a produtos com elementos digitais que sejam 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. As autoridades de fiscalização do mercado designadas nos termos do n.º 2 do presente artigo são igualmente responsáveis pela realização de atividades de fiscalização do mercado relacionadas com as obrigações dos administradores de *software* de código-fonte aberto estabelecidas no artigo 24.º. Caso uma autoridade de fiscalização do mercado constate que um administrador de *software* de código-fonte aberto não cumpre as obrigações estabelecidas no referido artigo, deve exigir que o administrador de *software* de código-fonte aberto assegure que sejam adotadas todas as medidas corretivas adequadas. Os administradores de *software* de código-fonte aberto devem assegurar que sejam adotadas todas as medidas corretivas adequadas no que se refere às suas obrigações decorrentes do presente regulamento.

4. Se for caso disso, as autoridades de fiscalização do mercado devem cooperar com as autoridades nacionais de certificação da cibersegurança designadas em conformidade com o 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 14.º do presente regulamento, as autoridades de fiscalização do mercado designadas devem cooperar e proceder regularmente a um intercâmbio de informações com as CSIRT designadas como coordenadoras e com a ENISA.

5. As autoridades de fiscalização do mercado podem solicitar à CSIRT designada como coordenadora ou à ENISA que preste aconselhamento técnico sobre questões relacionadas com a aplicação e a execução do presente regulamento. Ao realizarem uma investigação nos termos do artigo 54.º, as autoridades de fiscalização do mercado podem solicitar à CSIRT designada como coordenadora ou à ENISA que disponibilize uma análise para apoiar as avaliações não vinculativas da conformidade dos produtos com elementos digitais.

6. 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 que não o presente regulamento e proceder regularmente a um intercâmbio de informações.

7. 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 10, 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.

8. Os Estados-Membros devem assegurar que as autoridades de fiscalização do mercado designadas disponham dos recursos financeiros e técnicos adequados, incluindo, se for caso disso, ferramentas de tratamento automatizado, bem como dos recursos humanos dotados das competências necessárias em matéria de cibersegurança para exercerem as funções que lhes incumbem nos termos do presente regulamento.

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

10. As autoridades de fiscalização do mercado podem dar orientações e prestar aconselhamento aos operadores económicos sobre a execução do presente regulamento, com o apoio da Comissão e, se for caso disso, das CSIRT e da ENISA.

11. As autoridades de fiscalização do mercado devem informar os consumidores sobre o local onde devem apresentar reclamações que possam indicar um incumprimento do presente regulamento, em conformidade com o artigo 11.º do Regulamento (UE) 2019/1020, e devem facultar-lhes informações sobre os pontos e as modalidades de acesso a mecanismos para facilitar a comunicação de vulnerabilidades, incidentes e ciberameaças suscetíveis de afetar produtos com elementos digitais.

12. As autoridades de fiscalização do mercado devem facilitar, se for caso disso, a cooperação com as partes interessadas pertinentes, incluindo organizações científicas, de investigação e de consumidores.

13. 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.

14. No caso dos produtos com elementos digitais que são abrangidos pelo âmbito de aplicação do presente regulamento e que são classificados como sistemas de IA de risco elevado em conformidade com o artigo 6.º do Regulamento (UE) 2024/1689, as autoridades de fiscalização do mercado designadas para efeitos desse regulamento 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 (UE) 2024/1689 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 14.º do presente regulamento, com as CSIRT designadas como coordenadoras e com a ENISA. As autoridades de fiscalização do mercado designadas nos termos do Regulamento (UE) 2024/1689 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.

15. É criado o ADCO para a aplicação uniforme do presente regulamento, nos termos do artigo 30.º, n.º 2, do Regulamento (UE) 2019/1020. O ADCO é composto por representantes das autoridades de fiscalização do mercado designadas e, se for caso disso, representantes dos serviços de ligação únicos. O ADCO trata igualmente de matérias específicas das atividades de fiscalização do mercado relacionadas com as obrigações impostas aos administradores de *software* de código-fonte aberto.

16. As autoridades de fiscalização do mercado devem monitorizar a forma como os fabricantes aplicaram os critérios referidos no artigo 13.º, n.º 8, ao determinarem o período de apoio dos seus produtos com elementos digitais.

O ADCO publica, numa forma acessível ao público e de fácil utilização, estatísticas pertinentes sobre as categorias de produtos com elementos digitais, incluindo os períodos médios de apoio, conforme determinado pelo fabricante nos termos do artigo 13.º, n.º 8, bem como fornece orientações que incluam períodos de apoio indicativos para as categorias de produtos com elementos digitais.

Se os dados sugerirem períodos de apoio inadequados para categorias específicas de produtos com elementos digitais, o ADCO pode formular recomendações destinadas às autoridades de fiscalização do mercado para que estas centrem as suas atividades nessas categorias de produtos com elementos digitais.

Artigo 53.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 de cibersegurança constantes do anexo I, as autoridades de fiscalização do mercado devem, mediante pedido fundamentado, ser autorizadas a aceder, numa língua que compreendam facilmente, aos dados necessários para avaliar a conceção, o desenvolvimento, a produção e o tratamento de vulnerabilidades desses produtos, incluindo a documentação interna conexa do operador económico pertinente.

Artigo 54.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, sem demora injustificada e, se for caso disso, em cooperação com a CSIRT pertinente, avaliar esse produto no que diz respeito ao cumprimento de todos os requisitos previstos no presente regulamento. Os operadores económicos envolvidos devem cooperar com as autoridades de fiscalização do mercado conforme necessário.

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 elementos digitais com os requisitos mencionados, para o retirar do mercado ou para o recolher num prazo razoável que seja proporcional à natureza do risco de cibersegurança e que seja fixado pela autoridade de fiscalização do mercado.

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.

2. Ao determinar a importância do risco de cibersegurança referido no n.º 1 do presente artigo, as autoridades de fiscalização do mercado devem também ter em conta fatores de risco não técnicos, em especial os estabelecidos na sequência de avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas a nível da União realizadas em conformidade com o artigo 22.º da Diretiva (UE) 2022/2555. Se tiver motivos suficientes para considerar que um produto com elementos digitais apresenta um risco de cibersegurança significativo à luz de fatores de risco não técnicos, a autoridade de fiscalização do mercado deve informar as autoridades competentes designadas ou criadas nos termos do artigo 8.º da Diretiva (UE) 2022/2555 e cooperar com essas autoridades conforme necessário.

3. 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 económico tomasse.

4. Cabe ao operador económico 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.

5. Caso o operador económico 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 com elementos digitais nos seus mercados nacionais, para o retirar do mercado ou para o recolher.

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

6. A informação referida no n.º 5 deve conter todos os pormenores disponíveis, em especial os dados necessários à identificação do produto com elementos digitais não conforme, da origem desse 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 económico 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 com elementos digitais ou os processos aplicados pelo fabricante satisfazerem os requisitos essenciais de cibersegurança constantes do anexo I;

b) Lacunas das normas harmonizadas, dos sistemas europeus de certificação da cibersegurança ou das especificações comuns a que se refere o artigo 27.º.

7. 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 com elementos digitais em causa e, em caso de desacordo com a medida nacional notificada, das suas objeções.

8. Se, no prazo de três meses a contar da receção da notificação referida no n.º 5 do presente artigo, 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 económico em causa previstos no artigo 18.º do Regulamento (UE) 2019/1020.

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

Artigo 55.º

Procedimento de salvaguarda da União

1. Se, nos três meses subsequentes à receção da notificação a que se refere o artigo 54.º, n.º 5, um Estado-Membro levantar objeções a uma medida tomada por outro Estado-Membro, ou a Comissão considerar que a medida é contrária ao direito 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 54.º, n.º 5, 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 não for considerada justificada, 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 11.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 27.º, a Comissão deve ponderar a possibilidade de alterar ou revogar qualquer ato delegado adotado nos termos do artigo 27.º, n.º 9, 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 27.º, a Comissão deve ponderar a possibilidade de alterar ou revogar qualquer ato de execução adotado nos termos do artigo 27.º, n.º 2, que estabelece as referidas especificações comuns.

Artigo 56.º

Procedimento a nível da União 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 deve informar as autoridades de fiscalização do mercado competentes. Se as autoridades de fiscalização do mercado efetuarem uma avaliação desse produto com elementos digitais que possa apresentar um risco de cibersegurança significativo no que diz respeito à sua conformidade com os requisitos estabelecidos no presente regulamento, aplicam-se os procedimentos referidos nos artigos 54.º e 55.º.

2. Se tiver motivos suficientes para considerar que um produto com elementos digitais apresenta um risco de cibersegurança significativo à luz de fatores de risco não técnicos, a Comissão deve informar as autoridades de fiscalização do mercado pertinentes e, se for caso disso, as autoridades competentes designadas ou criadas nos termos do artigo 8.º da Diretiva (UE) 2022/2555 e cooperar com essas autoridades conforme necessário. A Comissão deve também analisar a pertinência dos riscos identificados para esse produto com elementos digitais, tendo em conta as suas atribuições no que diz respeito às avaliações coordenadas dos riscos de segurança das cadeias de abastecimento críticas a nível da União previstas no artigo 22.º da Diretiva (UE) 2022/2555, e consultar, se necessário, o grupo de cooperação criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555 e a ENISA.

3. Em circunstâncias que justifiquem uma intervenção imediata de modo a preservar o funcionamento adequado do mercado interno e se a Comissão tiver motivos suficientes para considerar que o produto com elementos digitais 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 procede a uma avaliação da conformidade e pode solicitar à ENISA que disponibilize uma análise para a apoiar. A Comissão deve informar desse facto as autoridades de fiscalização do mercado competentes. Os operadores económicos envolvidos devem cooperar com a ENISA conforme necessário.

4. Com base na avaliação referida no n.º 3, a Comissão pode decidir que é necessária uma medida corretiva ou restritiva a nível da União. Para esse efeito, deve consultar sem demora os Estados-Membros em causa e o operador ou operadores económicos em causa.

5. Com base na consulta referida no n.º 4 do presente artigo, a Comissão pode adotar atos de execução de forma a prever medidas corretivas ou restritivas a nível da União, incluindo requerer que os produtos com elementos digitais em causa sejam retirados do mercado ou recolhidos, 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 62.º, n.º 2.

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

7. Os n.ºs 3 a 6 devem ser aplicáveis durante o período de existência da situação excecional que justificou a intervenção da Comissão, desde que o respetivo produto com elementos digitais em causa não esteja em conformidade com o presente regulamento.

Artigo 57.º

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

1. A autoridade de fiscalização do mercado de um Estado-Membro deve exigir a um operador económico que tome todas as medidas adequadas sempre que, após ter efetuado uma avaliação nos termos do artigo 54.º, verificar que, embora um produto com elementos digitais e os processos aplicados pelo fabricante estejam em conformidade com o presente regulamento, estes apresentam um risco de cibersegurança significativo, bem como um risco para:

a) A saúde ou a segurança das pessoas;

b) O cumprimento de obrigações impostas pelo direito da União ou pelo direito nacional destinadas a proteger os direitos fundamentais;

c) A disponibilidade, a autenticidade, a integridade ou a confidencialidade dos serviços oferecidos através de um sistema de informação eletrónico pelas entidades essenciais a que se refere o artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555; ou

d) Outros aspetos da proteção do interesse público.

As medidas referidas no primeiro parágrafo podem incluir medidas destinadas a assegurar que o produto com elementos digitais em causa e os processos aplicados pelo fabricante já não apresentem os riscos pertinentes aquando da disponibilização no mercado, da retirada do mercado do produto com elementos digitais em causa ou da sua recolha, e devem ser proporcionais à natureza desses riscos.

2. O fabricante ou outros operadores económicos 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 referida no n.º 4.

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 do presente artigo, não obstante o facto de estar conforme com o presente regulamento, a Comissão deve informar a autoridade ou autoridades de fiscalização do mercado competentes e pode solicitar que efetuem uma avaliação e sigam os procedimentos referidos no artigo 54.º e nos n.ºs 1, 2 e 3 do presente artigo.

7. Em circunstâncias que justifiquem uma intervenção imediata de modo a preservar o funcionamento adequado do mercado interno, se tiver motivos suficientes para considerar que o produto com elementos digitais 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 deve proceder a uma avaliação dos riscos que o produto com elementos digitais em causa apresenta e pode solicitar à ENISA que disponibilize uma análise para apoiar essa avaliação, devendo informar desse facto as autoridades de fiscalização do mercado competentes. Os operadores económicos envolvidos devem cooperar com a ENISA conforme necessário.

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

9. Com base na consulta referida no n.º 8 do presente artigo, a Comissão pode adotar atos de execução de forma a decidir sobre medidas corretivas ou restritivas a nível da União, incluindo requerendo que os produtos com elementos digitais em causa sejam retirados do mercado ou recolhidos, 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 62.º, n.º 2.

10. A Comissão deve comunicar imediatamente os atos de execução referidos no n.º 9 ao operador ou operadores económicos em causa. Os Estados-Membros devem aplicar sem demora esses atos de execução 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 produto com elementos digitais em causa continuar a apresentar os riscos referidos no n.º 1.

Artigo 58.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 CE foi aposta em violação do disposto nos artigos 29.º e 30.º;

b) A marcação CE 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 no procedimento de avaliação da conformidade, se for caso disso, 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 59.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 no mercado ou disponibilizados no mercado, em especial produtos com elementos digitais que se constate frequentemente que apresentam riscos de cibersegurança.

2. A Comissão ou a ENISA devem 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 com elementos digitais que sejam abrangidos pelo âmbito de aplicação do presente regulamento com os requisitos estabelecidos no presente regulamento.

3. As autoridades de fiscalização do mercado e, se for caso disso, a Comissão 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 obtidas na sequência das atividades conjuntas realizadas no âmbito de uma investigação por si efetuada.

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

Artigo 60.º

Ações de fiscalização conjuntas

1. As autoridades de fiscalização do mercado devem realizar ações de controlo coordenadas simultâneas (ações de fiscalização conjuntas) de determinados produtos com elementos digitais ou categorias de tais produtos para verificar o cumprimento do presente regulamento ou detetar infrações ao mesmo. Essas ações de fiscalização conjuntas podem incluir inspeções de produtos com elementos digitais adquiridos sob uma identidade falsa.

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 deve, se for caso disso, colocar à disposição do público os resultados agregados.

3. Sempre que, no exercício das suas funções, nomeadamente com base nas notificações recebidas em conformidade com o artigo 14.º, n.ºs 1, e 3, a ENISA identificar as categorias de produtos com elementos digitais para as quais podem ser organizadas ações de fiscalização conjuntas, deve apresentar uma proposta de ação de fiscalização conjunta ao coordenador referido no n.º 2 do presente artigo, 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 52.º a 58.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 61.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 5, segundo parágrafo, no artigo 7.º, n.º 3, no artigo 8.º, n.ºs 1 e 2, no artigo 13.º, n.º 8, quarto parágrafo, no artigo 14.º, n.º 9, no artigo 25.º, no artigo 27.º, n.º 9, no artigo 28.º, n.º 5, e no artigo 31.º, n.º 5, é conferido à Comissão por um prazo de cinco anos a contar de 10 de dezembro de 2024. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

3. A delegação de poderes referida no artigo 2.º, n.º 5, segundo parágrafo, no artigo 7.º, n.º 3, no artigo 8.º, n.ºs 1 e 2, no artigo 13.º, n.º 8, quarto parágrafo, no artigo 14.º, n.º 9, no artigo 25.º, no artigo 27.º, n.º 9, no artigo 28.º, n.º 5, e no artigo 31.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, de 13 de abril de 2016, sobre legislar melhor.

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

6. Os atos delegados adotados nos termos do artigo 2.º, n.º 5, segundo parágrafo, do artigo 7.º, n.º 3, do artigo 8.º, n.ºs 1 ou 2, do artigo 13.º, n.º 8, quarto parágrafo, do artigo 14.º, n.º 9, do artigo 25.º, do artigo 27.º, n.º 9, do artigo 28.º, n.º 5, ou do artigo 31.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 62.º

Procedimento de comité

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

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

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

CAPÍTULO VII

CONFIDENCIALIDADE E SANÇÕES

Artigo 63.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 ([37]);

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 64.º

Sanções

1. Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação do disposto no presente regulamento e tomam todas as medidas necessárias para assegurar a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Os Estados-Membros notificam a Comissão, sem demora, dessas regras e dessas medidas e também, sem demora, de qualquer alteração ulterior.

2. A não conformidade com os requisitos essenciais de cibersegurança estabelecidos no anexo I e as obrigações previstas nos artigos 13.º e 14.º fica sujeita a coimas até 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.

3. A não conformidade com as obrigações previstas nos artigos 18.º a 23.º, no artigo 28.º, no artigo 30.º, n.os 1 a 4, no artigo 31.º, n.os 1 a 4, no artigo 32.º, n.os 1, 2 e 3, no artigo 33.º, n.º 5, e nos artigos 39.º, 41.º, 47.º, 49.º e 53.º, 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.

4. A prestação 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.

([37]) 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).

5. 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 as mesmas ou outras autoridades de fiscalização do mercado já aplicaram coimas ao mesmo operador económico por uma infração semelhante;

c) A dimensão, em particular no que diz respeito às microempresas e às pequenas e médias empresas, incluindo as empresas em fase de arranque, e a quota de mercado do operador económico que cometeu a infração.

6. As autoridades de fiscalização do mercado que aplicam coimas devem prestar informações sobre esta aplicação às 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.

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

8. 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.

9. 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.

10. Em derrogação dos n.os 3 a 9, as coimas previstas nesses números não se aplicam a:

a) Fabricantes que sejam considerados microempresas ou pequenas empresas no que diz respeito ao incumprimento do prazo referido no artigo 14.º, n.º 2, alínea a), ou no artigo 14.º, n.º 4, alínea a);

b) Qualquer infração ao presente regulamento por parte de administradores de *software* de código-fonte aberto.

Artigo 65.º

Ações coletivas

A Diretiva (UE) 2020/1828 é aplicável às ações coletivas intentadas contra infrações às disposições constantes do presente regulamento cometidas por operadores económicos que prejudiquem, ou sejam suscetíveis de prejudicar, os interesses coletivos dos consumidores.

CAPÍTULO VIII

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Artigo 66.º

Alteração do Regulamento (UE) 2019/1020

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

«72. Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho (*).

(*) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).».

Artigo 67.º

Alteração da Diretiva (UE) 2020/1828

Ao anexo I da Diretiva (UE) 2020/1828, é aditado o seguinte ponto:

«69) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho (*).

(*) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).».

Artigo 68.º

Alteração do Regulamento (UE) n.º 168/2013

À parte C1, no quadro, do anexo II do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho ([38]), é aditada a seguinte entrada:

«

16	18	Proteção de veículos contra ataques cibernéticos		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

»

Artigo 69.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 legislação de harmonização da União que não seja o presente regulamento permanecem válidos até 11 de junho de 2028, a menos que caduquem antes dessa data, ou salvo especificação em contrário nessa outra legislação de harmonização da União, caso em que permanecem válidos nos termos dessa legislação.

2. Os produtos com elementos digitais que tenham sido colocados no mercado antes de 11 de dezembro de 2027 só ficam sujeitos aos requisitos definidos no presente regulamento se, a partir dessa data, esses produtos forem objeto de uma modificação substancial.

3. Em derrogação do n.º 2 do presente artigo, as obrigações estabelecidas no artigo 14.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 11 de dezembro de 2027.

Artigo 70.º

Avaliação e reexame

1. Até 11 de dezembro de 2030 e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e o reexame do presente regulamento. Esses relatórios devem ser divulgados ao público.

2. Até 11 de setembro de 2028, a Comissão, após consulta da ENISA e da rede de CSIRT, apresenta ao Parlamento Europeu e ao Conselho um relatório que avalie a eficácia da plataforma única de comunicação prevista no artigo 16.º, bem como o impacto da aplicação dos motivos relacionados com a cibersegurança, a que se refere o artigo 16.º, n.º 2, pelas CSIRT designadas como coordenadores na eficácia da plataforma única de comunicação no que diz respeito à divulgação atempada das notificações recebidas a outras CSIRT pertinentes.

Artigo 71.º

Entrada em vigor e aplicação

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

([38]) Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52).

2. O presente regulamento é aplicável a partir de 11 de dezembro de 2027.

Todavia, o artigo 14.º é aplicável a partir de 11 de setembro de 2026 e o capítulo IV (artigos 35.º a 51.º) é aplicável a partir de 11 de junho de 2026.

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

Feito em Estrasburgo, em 23 de outubro de 2024.

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*
R. METSOLA	ZSIGMOND B. P.

ANEXO I

REQUISITOS ESSENCIAIS DE CIBERSEGURANÇA

Parte I Requisitos de cibersegurança relativos às propriedades dos produtos com elementos digitais

1) Os produtos com elementos digitais devem ser concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança com base nos riscos.

2) Com base na avaliação dos riscos de cibersegurança referida no artigo 13.º, n.º 2, e se for caso disso, os produtos com elementos digitais devem:

   a) Ser disponibilizados no mercado sem nenhuma vulnerabilidade passível de ser explorada conhecida;

   b) Ser disponibilizados no mercado com uma configuração segura por defeito, salvo acordo em contrário entre o fabricante e o utilizador profissional em relação a um produto personalizado com elementos digitais, incluindo a possibilidade de restaurar o produto para o seu estado original;

   c) Assegurar que as vulnerabilidades possam ser corrigidas através de atualizações de segurança, incluindo, se for caso disso, atualizações de segurança automáticas, instaladas num prazo adequado, configuradas por defeito, com um mecanismo de autoexclusão claro e de fácil utilização, por meio da notificação das atualizações disponíveis aos utilizadores e com a opção de as adiar temporariamente;

   d) Assegurar a proteção contra o acesso não autorizado através de mecanismos de controlo adequados, incluindo, nomeadamente, sistemas de autenticação, identidade ou gestão de acessos, e comunicar eventuais acessos não autorizados;

   e) Proteger a confidencialidade dos dados armazenados, transmitidos ou tratados de outra forma, sejam eles pessoais ou de outra natureza, por exemplo através da cifragem de dados inativos ou em trânsito pertinentes por mecanismos de ponta e da utilização de outros meios técnicos;

   f) Proteger a integridade dos dados armazenados, transmitidos ou tratados de outra forma, sejam eles pessoais ou de outra natureza, dos comandos, dos programas e da configuração contra qualquer manipulação ou modificação não autorizada pelo utilizador, e comunicar informações sobre as corrupções;

   g) Tratar apenas dados, pessoais ou de outra natureza, que sejam adequados, pertinentes e limitados ao que é necessário para a finalidade prevista do produto com elementos digitais (minimização de dados);

   h) Proteger a disponibilidade de funções essenciais e básicas, inclusivamente após um incidente, incluindo através de medidas de resiliência e atenuação contra-ataques de negação de serviço;

   i) Minimizar o impacto negativo pelos próprios produtos ou dispositivos conectados na disponibilidade de serviços prestados por outros dispositivos ou redes;

   j) Ser concebidos, desenvolvidos e produzidos de forma a limitar superfícies de ataque, incluindo interfaces externas;

   k) Ser concebidos, desenvolvidos e produzidos de forma a reduzir o impacto de incidentes, utilizando mecanismos e técnicas adequados de atenuação da exploração;

   l) Facultar informações relacionadas com a segurança através do registo e controlo da atividade interna pertinente, incluindo o acesso ou a alteração de dados, serviços ou funções, com um mecanismo de autoexclusão para o utilizador;

   m) Prever a possibilidade de os utilizadores removerem de forma segura, fácil e permanente todos os dados e parâmetros e, nos casos em que esses dados possam ser transferidos para outros produtos ou sistemas, assegurar que tal é feito de forma segura.

Parte II Requisitos de tratamento de vulnerabilidades

Os fabricantes de produtos com elementos digitais devem:

1) Identificar e documentar vulnerabilidades e componentes existentes nos produtos com elementos digitais, nomeadamente elaborando uma lista de materiais do *software* num formato de uso corrente e legível por máquina que abranja, pelo menos, as dependências de nível superior dos produtos;

2) Em relação aos riscos que os produtos com elementos digitais enfrentam, resolver e corrigir, sem demora, as vulnerabilidades, nomeadamente disponibilizando atualizações de segurança; sempre que tecnicamente viável, devem ser fornecidas novas atualizações de segurança, distintas das atualizações das funcionalidades;

3) Efetuar ensaios e análises eficazes e regulares da segurança do produto com elementos digitais;

4) Uma vez disponibilizada uma atualização de segurança, partilhar e divulgar publicamente informações sobre as vulnerabilidades corrigidas, incluindo uma descrição das mesmas, informações que permitam aos utilizadores identificar o produto com elementos digitais afetado, os impactos das vulnerabilidades, a sua gravidade e informações claras e acessíveis, que ajudem os utilizadores a corrigir as vulnerabilidades; em casos devidamente justificados, sempre que os fabricantes considerem que os riscos de segurança da publicação superam os benefícios relacionados com a segurança, podem adiar a divulgação pública de informações sobre uma vulnerabilidade corrigida até que os utilizadores tenham a possibilidade de aplicar a correção pertinente;

5) Definir e aplicar uma política de divulgação coordenada de vulnerabilidades;

6) Tomar medidas para facilitar a partilha de informações sobre potenciais vulnerabilidades no seu produto com elementos digitais, bem como em componentes de terceiros incluídos nesse produto, nomeadamente facultando um endereço de contacto para a comunicação das vulnerabilidades detetadas no produto com elementos digitais;

7) Prever mecanismos para distribuir de forma segura as atualizações de produtos com elementos digitais, a fim de assegurar a correção ou atenuação das vulnerabilidades em tempo útil e, se aplicável às atualizações de segurança, de uma forma automática;

8) Assegurar que as atualizações de segurança disponíveis para resolver problemas de segurança identificados sejam distribuídas sem demora e, salvo acordo em contrário entre um fabricante e um utilizador profissional em relação a um produto personalizado com elementos digitais, de forma gratuita, juntamente com orientações que facultem aos utilizadores informações pertinentes, nomeadamente sobre as eventuais medidas a tomar.

ANEXO II

INFORMAÇÕES E INSTRUÇÕES DESTINADAS AO UTILIZADOR

No mínimo, devem ser facultadas com o produto com elementos digitais as seguintes indicações:

1. O nome, nome comercial registado ou marca registada do fabricante, bem como o seu endereço postal, o endereço de correio eletrónico ou outro contacto digital e, se existir, o sítio Web através do qual o fabricante pode ser contactado;
2. O ponto de contacto único por meio do qual se pode comunicar e receber informações sobre vulnerabilidades do produto com elementos digitais e a política do fabricante em matéria de divulgação coordenada das vulnerabilidades;
3. Nome e tipo do produto com elementos digitais, bem como quaisquer informações complementares que permitam a sua identificação única;
4. A finalidade prevista do produto com elementos digitais, incluindo o ambiente de segurança proporcionado pelo fabricante, bem como as funcionalidades essenciais do produto e informações sobre as propriedades de segurança;
5. Qualquer circunstância conhecida ou previsível, relacionada com a utilização do produto com elementos digitais de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível que possam dar origem a riscos de cibersegurança significativos;
6. Se for caso disso, o endereço Internet que permite aceder à declaração de conformidade UE;
7. O tipo de apoio técnico no domínio da segurança que o fabricante oferece e a data-limite do período de apoio durante o qual os utilizadores podem esperar que as vulnerabilidades sejam tratadas e receber atualizações de segurança;
8. Instruções pormenorizadas ou um endereço Internet que remeta para tais instruções pormenorizadas e informações sobre:
   a) As medidas a tomar quando o produto com elementos digitais é posto em funcionamento pela primeira vez e ao longo de toda a sua vida útil de modo a garantir uma utilização segura do mesmo;
   b) Como as alterações do produto com elementos digitais podem afetar a segurança dos dados;
   c) Como podem ser instaladas atualizações relevantes em termos de segurança;
   d) A desativação segura do produto com elementos digitais, incluindo informações sobre como se pode remover de forma segura os dados dos utilizadores.
   e) A forma como pode ser desligada a configuração por defeito que permite a instalação automática de atualizações de segurança, conforme exigido pela parte I, ponto 2, alínea c), do anexo I;
   f) Se o produto com elementos digitais se destinar a ser integrado noutros produtos com elementos digitais, as informações necessárias para que o responsável pela integração cumpra os requisitos essenciais de cibersegurança estabelecidos no anexo I e os requisitos em matéria de documentação estabelecidos no anexo VII.
9. Se o fabricante decidir disponibilizar a lista de materiais de *software* ao utilizador, informações sobre o local onde se pode aceder à lista de materiais do *software*.

ANEXO III

PRODUTOS IMPORTANTES COM ELEMENTOS DIGITAIS

Classe I

1. Sistemas de gestão de identidade e *software* e *hardware* de gestão de acesso privilegiado, nomeadamente leitores de autenticação e controlo do acesso, incluindo leitores biométricos
2. Navegadores autónomos e incorporados
3. Gestores de senhas
4. *Software* de pesquisa, remoção ou colocação em quarentena de *software* malicioso
5. Produtos com elementos digitais com a função de rede privada virtual (VPN)
6. Sistemas de gestão de rede
7. Sistemas de gestão de informações e eventos de segurança (SIEM)
8. Gestores de arranque
9. Infraestruturas de chaves públicas e *software* de emissão de certificados digitais
10. Interfaces físicas e virtuais da rede
11. Sistemas operativos
12. Encaminhadores, modems para ligação à Internet e comutadores
13. Microprocessadores com funcionalidades relacionadas com a cibersegurança
14. Microcontroladores com funcionalidades relacionadas com a cibersegurança
15. Circuitos integrados de aplicação específica (ASIC) e redes de portas lógicas programáveis (FPGA) com funcionalidades relacionadas com a cibersegurança
16. Assistentes virtuais de uso geral para residências inteligentes
17. Produtos domésticos inteligentes com funcionalidades de segurança, incluindo fechaduras inteligentes, câmaras de segurança, sistemas de monitorização de bebés e sistemas de alarme
18. Brinquedos ligados à Internet, abrangidos pela Diretiva 2009/48/CE do Parlamento Europeu e do Conselho [1], com características sociais interativas (por exemplo, que falam ou filmam) ou que têm características de localização
19. Produtos pessoais usáveis, para usar ou colocar no corpo humano, destinados à monitorização do estado de saúde (p. ex., rastreio) e aos quais não se aplicam o Regulamento (UE) 2017/745 ou (UE) 2017/746, ou produtos pessoais usáveis, a utilizar por crianças ou a estas destinados

Classe II

1. Hipervisores e sistemas *container runtime* que permitam a execução virtualizada de sistemas operativos e ambientes semelhantes
2. Barreiras de segurança, sistemas de deteção e prevenção de intrusões
3. Microprocessadores invioláveis
4. Microcontroladores invioláveis

[1] Diretiva 2009/48/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009, relativa à segurança dos brinquedos (JO L 170 de 30.6.2009, p. 1).

ANEXO IV

PRODUTOS CRÍTICOS COM ELEMENTOS DIGITAIS

1. Dispositivos de *hardware* com caixas de segurança
2. Pontos de acesso para contadores inteligentes no âmbito de sistemas de contadores inteligentes, conforme definidos no artigo 2.º, ponto 23, da Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho ([1]), e outros dispositivos para fins avançados de segurança, incluindo o criptoprocessamento seguro
3. Cartões inteligentes ou dispositivos semelhantes, incluindo elementos seguros

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

ANEXO V

DECLARAÇÃO DE CONFORMIDADE UE

A declaração de conformidade UE referida no artigo 28.º deve conter todas as seguintes informações:

1. Nome e tipo do produto com elementos digitais, bem como quaisquer informações complementares que permitam a sua identificação única
2. Nome e endereço do fabricante ou do respetivo mandatário
3. Menção de que a declaração de conformidade UE é emitida sob a exclusiva responsabilidade do fornecedor
4. Objeto da declaração (identificação do produto com elementos digitais que permita rastreá-lo, podendo incluir uma fotografia, se for caso disso)
5. Menção de que o objeto da declaração acima mencionado está em conformidade com a legislação de harmonização da União aplicável
6. Referências a quaisquer normas harmonizadas pertinentes aplicadas ou a quaisquer outras especificações comuns ou certificações da cibersegurança em relação às quais é declarada a conformidade
7. Se for caso disso, nome e número do organismo notificado, descrição do procedimento de avaliação da conformidade efetuado e identificação do certificado emitido
8. Informações complementares:

   Assinado em nome de:

   (local e data de emissão):

   (nome, cargo) (assinatura):

ANEXO VI

DECLARAÇÃO DE CONFORMIDADE UE SIMPLIFICADA

A declaração de conformidade UE simplificada a que se refere o artigo 13.º, n.º 20, deve conter os seguintes dados:

Pela presente, … [*nome do fabricante*] declara que o tipo de produto com elementos digitais … [*designação do tipo de produto com elemento digital*] está em conformidade com o Regulamento (UE) 2024/2847 ([1]).

O texto integral da declaração de conformidade UE está disponível no seguinte endereço eletrónico: …

([1]) JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

ANEXO VII

TEOR DA DOCUMENTAÇÃO TÉCNICA

A documentação técnica referida no artigo 31.º deve incluir, pelo menos, as informações indicadas a seguir, consoante aplicável ao produto com elementos digitais em causa:

1. Uma descrição geral do produto com elementos digitais, incluindo:
   a) A sua finalidade prevista;
   b) Versões do *software* suscetíveis de afetar a conformidade com os requisitos essenciais de cibersegurança;
   c) Se o produto com elementos digitais for um produto de *hardware*, fotografias ou ilustrações que mostrem as características externas, a marcação e a disposição interna;
   d) Informações e instruções destinadas aos utilizadores, conforme consta do anexo II;
2. Uma descrição da conceção, do desenvolvimento, da produção do produto com elementos digitais e dos processos de tratamento de vulnerabilidades, incluindo:
   a) Informações necessárias sobre a conceção e o desenvolvimento do produto com elementos digitais, incluindo, se for caso disso, ilustrações e esquemas e uma descrição da arquitetura do sistema que explique de que forma os componentes de *software* se apoiam ou se alimentam mutuamente e se integram no processamento global;
   b) Informações e especificações necessárias sobre os processos de tratamento de vulnerabilidades aplicados pelo fabricante, incluindo a lista de materiais do *software*, a política de divulgação coordenada de vulnerabilidades, comprovativos da disponibilização de um endereço de contacto para a comunicação de vulnerabilidades e uma descrição das soluções técnicas escolhidas para a distribuição segura de atualizações;
   c) Informações e especificações necessárias sobre os processos de produção e controlo do produto com elementos digitais e a validação desses processos;
3. Uma avaliação dos riscos de cibersegurança tidos em conta na conceção, no desenvolvimento, na produção, na entrega e na manutenção do produto com elementos digitais, nos termos do artigo 13.º, incluindo a forma como são aplicáveis os requisitos essenciais de cibersegurança estabelecidos na parte I do anexo I;
4. Informações pertinentes tidas em conta para determinar o período de apoio nos termos do artigo 13.º, n.º 8, do produto com elementos digitais;
5. Uma lista das normas harmonizadas aplicadas total ou parcialmente, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, das especificações comuns previstas no artigo 27.º do presente regulamento ou dos sistemas europeus de certificação da cibersegurança adotados ao abrigo do Regulamento (UE) 2019/881, nos termos do artigo 27.º, n.º 8, do presente regulamento e, nos casos em que essas normas harmonizadas, especificações comuns ou sistemas europeus de certificação da cibersegurança não tenham sido aplicados, uma descrição das soluções adotadas para dar cumprimento aos requisitos essenciais de cibersegurança estabelecidos nas partes I e II do anexo I, incluindo uma lista de outras especificações técnicas pertinentes aplicadas. Em caso de aplicação parcial das normas harmonizadas, das especificações comuns ou dos sistemas europeus de certificação da cibersegurança, a documentação técnica deve especificar as partes que foram aplicadas;
6. Relatórios dos ensaios realizados para verificar a conformidade do produto com elementos digitais e dos processos de tratamento de vulnerabilidades com os requisitos essenciais de cibersegurança aplicáveis estabelecidos nas partes I e II do anexo I;
7. Uma cópia da declaração de conformidade UE;
8. Se for caso disso, a lista de materiais do *software*, na sequência de um pedido fundamentado de uma autoridade de fiscalização do mercado, desde que tal seja necessário para que a referida autoridade possa verificar a conformidade com os requisitos essenciais de cibersegurança estabelecidos no anexo I.

ANEXO VIII

PROCEDIMENTOS DE AVALIAÇÃO DA CONFORMIDADE

Parte I Procedimento de avaliação da conformidade baseado no controlo interno (com base no módulo A)

1. O controlo interno é o procedimento de avaliação da conformidade mediante o qual o fabricante cumpre as obrigações estabelecidas nos pontos 2, 3 e 4 da presente parte e garante e declara, sob a sua exclusiva responsabilidade, que os produtos com elementos digitais cumprem todos os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e que o fabricante cumpre os requisitos essenciais de cibersegurança estabelecidos na parte II do anexo I.

2. O fabricante deve elaborar a documentação técnica descrita no anexo VII.

3. Conceção, desenvolvimento, produção e tratamento de vulnerabilidades de produtos com elementos digitais

   O fabricante deve tomar todas as medidas necessárias para que os processos de conceção, desenvolvimento, produção e tratamento de vulnerabilidades, bem como o respetivo controlo, assegurem a conformidade dos produtos com elementos digitais fabricados ou desenvolvidos e dos processos aplicados pelo fabricante com os requisitos essenciais de cibersegurança previstos nas partes I e II do anexo I.

4. Marcação de conformidade e declaração de conformidade

   4.1. O fabricante deve apor a marcação CE em cada produto com elementos digitais que cumpra os requisitos aplicáveis previstos no presente regulamento.

   4.2. O fabricante deve elaborar uma declaração de conformidade UE escrita para cada produto com elementos digitais nos termos do artigo 28.º e mantê-la, juntamente com a documentação técnica, à disposição das autoridades nacionais, por um período de 10 anos a contar da data de colocação no mercado do produto com elementos digitais ou durante período de apoio, consoante o que for mais longo. A declaração de conformidade UE deve identificar o produto com elementos digitais para o qual foi elaborada. Deve ser fornecida cópia da declaração de conformidade UE às autoridades competentes, a seu pedido.

5. Mandatários

   As obrigações do fabricante enunciadas no ponto 4 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo seu mandatário, desde que as obrigações pertinentes se encontrem especificadas no mandato.

Parte II Exame UE de tipo (com base no módulo B)

1. O exame UE de tipo é a parte do procedimento de avaliação da conformidade em que um organismo notificado examina o projeto técnico e o desenvolvimento de um produto com elementos digitais, bem como os processos de tratamento de vulnerabilidades aplicados pelo fabricante, e certifica que um produto com elementos digitais cumpre os requisitos essenciais de cibersegurança estabelecidos na parte I do anexo I, e que o fabricante cumpre os requisitos essenciais de cibersegurança estabelecidos na parte II do anexo I.

2. O exame UE de tipo deve ser realizado através da avaliação da adequação do projeto técnico e do desenvolvimento do produto com elementos digitais mediante análise da documentação técnica e dos elementos de prova referidos no ponto 3, bem como do exame de amostras de uma ou mais partes críticas do produto (combinação de tipo de produção e tipo de projeto).

3. O fabricante deve apresentar o pedido de exame UE de tipo a um único organismo notificado da sua escolha.

   O pedido deve incluir os seguintes elementos:

   3.1. o nome e o endereço do fabricante e, se for apresentado pelo mandatário, o nome e o endereço deste último,

   3.2. uma declaração por escrito indicando que o mesmo pedido não foi apresentado a nenhum outro organismo notificado,

   3.3. a documentação técnica, que deve permitir avaliar a conformidade do produto com elementos digitais com os requisitos essenciais de cibersegurança aplicáveis constantes da parte I do anexo I, e os processos de tratamento de vulnerabilidades do fabricante constantes da parte II do anexo I, e deve incluir uma análise e uma avaliação adequadas dos riscos. A documentação técnica deve especificar os requisitos aplicáveis e abranger, se tal for pertinente para efeitos de avaliação, a conceção, o fabrico e o funcionamento do produto com elementos digitais. A documentação técnica deve conter, se for caso disso, pelo menos os elementos previstos no anexo VII,

3.4. os elementos de prova da adequação das soluções de projeto técnico e desenvolvimento e dos processos de tratamento de vulnerabilidades. Esses elementos devem fazer menção aos documentos utilizados, designadamente nos casos em que não foram integralmente aplicadas as normas harmonizadas ou as especificações técnicas pertinentes. Os elementos de prova devem incluir, se necessário, os resultados dos ensaios realizados pelo laboratório competente do fabricante ou por qualquer outro laboratório de ensaios em nome e sob a responsabilidade do fabricante.

4. O organismo notificado deve:

4.1. Examinar a documentação técnica e os elementos de prova para avaliar a adequação do projeto técnico e do desenvolvimento do produto com elementos digitais aos requisitos essenciais de cibersegurança constantes da parte I do anexo I, e a adequação dos processos de tratamento de vulnerabilidades aplicados pelo fabricante aos requisitos essenciais de cibersegurança estabelecidos na parte II do anexo I;

4.2. Verificar se as amostras foram desenvolvidas ou fabricadas em conformidade com a documentação técnica e identificar os elementos concebidos e desenvolvidos de acordo com as disposições aplicáveis das normas harmonizadas ou especificações técnicas pertinentes, bem como os elementos cuja conceção e desenvolvimento não se baseiem nas disposições pertinentes dessas normas;

4.3. Realizar, ou mandar realizar, os exames e os ensaios adequados para verificar que, caso o fabricante tenha optado pelas soluções constantes das normas harmonizadas ou especificações técnicas pertinentes para os requisitos previstos no anexo I, essas soluções foram corretamente aplicadas;

4.4. Realizar, ou mandar realizar, os exames e ensaios necessários para verificar que, caso as soluções constantes das normas harmonizadas ou especificações técnicas pertinentes para os requisitos previstos no anexo I não tenham sido aplicadas, as soluções adotadas pelo fabricante cumprem os requisitos essenciais de cibersegurança correspondentes;

4.5. Acordar com o fabricante o local de realização dos exames e dos ensaios.

5. O organismo notificado deve elaborar um relatório de avaliação que indique as atividades desenvolvidas de acordo com o ponto 4 e os respetivos resultados. Sem prejuízo das suas obrigações para com as autoridades notificadoras, o organismo notificado só pode divulgar, no todo ou em parte, o conteúdo desse relatório com o acordo do fabricante.

6. Se o tipo e os processos de tratamento de vulnerabilidades cumprirem os requisitos essenciais de cibersegurança constantes do anexo I, o organismo notificado deve remeter ao fabricante um certificado de exame UE de tipo. O certificado deve conter o nome e o endereço do fabricante, as conclusões do exame, as condições (se as houver) da sua validade e os dados necessários à identificação do tipo aprovado e dos processos de tratamento de vulnerabilidades. O certificado pode ser acompanhado de um ou mais anexos.

O certificado e os seus anexos devem conter todas as informações necessárias para permitir a avaliação da conformidade dos produtos com elementos digitais fabricados ou desenvolvidos com o tipo e os processos de tratamento de vulnerabilidades examinados e para permitir o controlo em serviço.

Nos casos em que o tipo e os processos de tratamento de vulnerabilidades não cumpram os requisitos essenciais de cibersegurança aplicáveis constantes do anexo I, o organismo notificado deve recusar emitir um certificado de exame UE de tipo e deve informar o requerente desse facto, fundamentando pormenorizadamente as razões da sua recusa.

7. O organismo notificado deve manter-se a par das alterações do estado da técnica geralmente reconhecido que indiquem que o tipo aprovado e os processos de tratamento de vulnerabilidades podem ter deixado de cumprir os requisitos essenciais de cibersegurança aplicáveis constantes do anexo I e deve determinar se tais alterações requerem exames complementares. Em caso afirmativo, o organismo notificado deve informar o fabricante desse facto.

O fabricante deve informar o organismo notificado que possui a documentação técnica relativa ao certificado de exame UE de tipo de todas as modificações do tipo aprovado e dos processos de tratamento de vulnerabilidades que possam afetar a conformidade com os requisitos essenciais de cibersegurança constantes do anexo I ou as condições de validade do certificado. Tais modificações devem ser objeto de aprovação complementar, na forma de aditamento ao certificado original de exame UE de tipo.

8. O organismo notificado deve efetuar auditorias periódicas para assegurar que os processos de tratamento das vulnerabilidades previstos na parte II do anexo I, são aplicados de forma adequada.

9. O organismo notificado deve informar as autoridades notificadoras dos certificados de exame UE de tipo e respetivos aditamentos que emitiu ou retirou e fornecer-lhes periodicamente, ou mediante pedido, a lista dos certificados e respetivos aditamentos recusados, suspensos ou objeto de restrições.

   Cada organismo notificado deve informar os outros organismos notificados dos certificados de exame UE de tipo e respetivos aditamentos que tenha recusado, retirado, suspendido ou submetido a quaisquer outras restrições e, mediante pedido, dos certificados que tenha emitido e dos aditamentos que tenha introduzido nos mesmos.

   A Comissão, os Estados-Membros e os outros organismos notificados podem, mediante pedido, obter cópia dos certificados de exame UE de tipo e quaisquer aditamentos. Mediante pedido, a Comissão e os Estados-Membros podem obter cópia da documentação técnica e dos resultados dos exames efetuados pelo organismo notificado. O organismo notificado deve conservar uma cópia do certificado de exame UE de tipo e dos respetivos anexos e aditamentos, assim como do processo técnico, incluindo a documentação apresentada pelo fabricante, até ao termo da validade do certificado.

10. O fabricante deve manter à disposição das autoridades nacionais uma cópia do certificado de exame UE de tipo e dos respetivos anexos e aditamentos, assim como da documentação técnica, por um período de 10 anos a contar da data de colocação do produto com elementos digitais no mercado ou durante o período de apoio, consoante o que for mais longo.

11. O mandatário do fabricante pode apresentar o pedido referido no ponto 3 e cumprir as obrigações previstas nos pontos 7 e 10, desde que as obrigações pertinentes se encontrem especificadas no mandato.

Parte III Conformidade com o tipo baseada no controlo interno da produção (com base no módulo C)

1. A conformidade com o tipo baseada no controlo interno da produção é a parte do procedimento de avaliação da conformidade mediante a qual o fabricante cumpre as obrigações previstas nos pontos 2 e 3 da presente parte e garante e declara que os produtos com elementos digitais em causa estão em conformidade com o tipo descrito no certificado de exame UE de tipo e satisfazem os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e que o fabricante cumpre os requisitos essenciais de cibersegurança estabelecidos na parte II do anexo I.

2. Produção

   O fabricante deve tomar todas as medidas necessárias para que a produção e o respetivo controlo garantam a conformidade dos produtos fabricados com o tipo aprovado descrito no certificado de exame UE de tipo e com os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e garante que o fabricante cumpre os requisitos essenciais de cibersegurança estabelecidos na parte II do anexo I.

3. Marcação de conformidade e declaração de conformidade

   3.1. O fabricante deve apor a marcação CE em cada produto com elementos digitais que esteja em conformidade com o tipo descrito no certificado de exame UE de tipo e que cumpra os requisitos aplicáveis definidos no presente regulamento.

   3.2. O fabricante deve elaborar uma declaração de conformidade escrita para cada modelo de produto e mantê-la à disposição das autoridades nacionais, por um período de 10 anos a contar da data de colocação do produto com elementos digitais no mercado ou durante o período de apoio, consoante o que for mais longo. A declaração de conformidade deve identificar o modelo de produto para o qual foi elaborada. Deve ser fornecida às autoridades competentes, a pedido destas, uma cópia da declaração de conformidade.

4. Mandatário

   As obrigações do fabricante enunciadas no ponto 3 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo seu mandatário, desde que as obrigações pertinentes se encontrem especificadas no mandato.

Parte IV Conformidade baseada na garantia de qualidade total (com base no módulo H)

1. A conformidade baseada na garantia de qualidade total é o procedimento de avaliação da conformidade mediante o qual o fabricante cumpre as obrigações estabelecidas nos pontos 2 e 5 da presente parte e garante e declara, sob a sua exclusiva responsabilidade, que os produtos com elementos digitais ou as categorias de produtos em causa cumprem os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e que os processos de tratamento de vulnerabilidades por si aplicados cumprem os requisitos estabelecidos na parte II do anexo I.

2. Conceção, desenvolvimento, produção e tratamento de vulnerabilidades de produtos com elementos digitais

O fabricante deve aplicar um sistema de qualidade aprovado, nos termos do ponto 3, para a conceção, o desenvolvimento e a inspeção e o ensaio dos produtos com elementos digitais em causa e para o tratamento de vulnerabilidades, deve manter a sua eficácia durante todo o período de apoio e fica sujeito à fiscalização prevista no ponto 4.

3. Sistema de qualidade

3.1. O fabricante deve apresentar um pedido de avaliação do seu sistema de qualidade para os produtos com elementos digitais em causa a um organismo notificado da sua escolha.

O pedido deve incluir os seguintes elementos:

a) o nome e o endereço do fabricante e, se for apresentado pelo mandatário, o nome e o endereço deste último;

b) a documentação técnica para um modelo de cada categoria de produtos com elementos digitais que se pretende fabricar ou desenvolver. A documentação técnica deve conter, no mínimo, se aplicável, os elementos previstos no anexo VII;

c) a documentação relativa ao sistema de qualidade; e

d) uma declaração escrita indicando que o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2. O sistema de qualidade deve assegurar a conformidade dos produtos com elementos digitais com os requisitos essenciais de cibersegurança constantes da parte I do anexo I, e a conformidade dos processos de tratamento de vulnerabilidades aplicados pelo fabricante com os requisitos estabelecidos na parte II do anexo I.

Todos os elementos, requisitos e disposições adotados pelo fabricante devem ser documentados de modo sistemático e ordenado, sob a forma de políticas, procedimentos e instruções escritas. A documentação relativa ao sistema de qualidade deve permitir uma interpretação coerente dos programas, planos, manuais e registos de qualidade.

Em especial, deve conter uma descrição adequada do seguinte:

a) objetivos de qualidade e estrutura organizativa, responsabilidades e competências dos órgãos de gestão no que diz respeito à conceção, ao desenvolvimento, à qualidade do produto e ao tratamento de vulnerabilidades;

b) especificações do projeto técnico e do desenvolvimento, incluindo as normas que serão aplicadas e, se as normas harmonizadas e/ou as especificações técnicas pertinentes não forem integralmente aplicadas, os meios a utilizar para assegurar o cumprimento dos requisitos essenciais de cibersegurança constantes da parte I do anexo I, aplicáveis aos produtos com elementos digitais;

c) especificações processuais, incluindo as normas que serão aplicadas e, se as normas harmonizadas ou as especificações técnicas pertinentes não forem integralmente aplicadas, os meios a utilizar para assegurar o cumprimento dos requisitos essenciais de cibersegurança constantes da parte II do anexo I, aplicáveis ao fabricante;

d) o controlo da conceção e do desenvolvimento, bem como as técnicas, os processos e as ações sistemáticas de verificação da conceção e do desenvolvimento a adotar ao conceber e desenvolver os produtos com elementos digitais pertencentes à categoria abrangida;

e) as técnicas, processos e ações sistemáticas de produção, controlo da qualidade e garantia da qualidade a aplicar correspondentes;

f) exames e ensaios a executar antes, durante e após a produção, e a frequência com que serão realizados;

g) os registos de qualidade, como relatórios de inspeções e dados dos ensaios, dados de calibração e relatórios de qualificação do pessoal envolvido, etc.;

h) meios que permitam controlar a obtenção da qualidade exigida ao nível da conceção e do produto, bem como a eficácia do funcionamento do sistema de qualidade.

3.3. O organismo notificado deve avaliar o sistema de qualidade para determinar se este satisfaz os requisitos referidos no ponto 3.2.

O organismo notificado deve presumir que são conformes com esses requisitos os elementos do sistema de qualidade que cumpram as especificações correspondentes da norma nacional que transpõe a norma harmonizada ou as especificações técnicas aplicáveis.

Para além de experiência em sistemas de gestão da qualidade, o grupo de auditores deve incluir pelo menos um membro com experiência como assessor no domínio pertinente do produto e na tecnologia do produto em causa e ter conhecimento dos requisitos aplicáveis previstos no presente regulamento. A auditoria deve incluir uma visita de avaliação às instalações do fabricante, no caso de estas existirem. O grupo de auditores deve analisar a documentação técnica referida no ponto 3.1, alínea b), para verificar a capacidade de o fabricante identificar os requisitos aplicáveis previstos no presente regulamento e realizar os exames necessários, com vista a assegurar a conformidade do produto com elementos digitais com esses requisitos.

A decisão deve ser notificada ao fabricante ou ao respetivo mandatário.

A notificação deve conter as conclusões da auditoria e a decisão de avaliação fundamentada.

3.4. O fabricante compromete-se a cumprir as obrigações decorrentes do sistema de qualidade aprovado e a assegurar que permanece adequado e eficaz.

3.5. O fabricante mantém informado o organismo notificado que tiver aprovado o sistema de qualidade de qualquer alteração planeada para o referido sistema.

O organismo notificado deve avaliar as alterações propostas e decidir se o sistema da qualidade alterado continua a satisfazer os requisitos referidos no ponto 3.2 ou se é necessária uma reavaliação.

O organismo notificado deve notificar o fabricante da sua decisão. A notificação deve conter as conclusões do exame e a decisão de avaliação fundamentada.

4. Fiscalização sob a responsabilidade do organismo notificado

4.1. O objetivo da fiscalização é garantir que o fabricante cumpre devidamente as obrigações decorrentes do sistema de qualidade aprovado.

4.2. O fabricante deve permitir o acesso do organismo notificado, para fins de avaliação, aos locais de conceção, desenvolvimento, produção, inspeção, ensaio e armazenamento, e facultar-lhe todas as informações necessárias, em especial:

a) a documentação relativa ao sistema de qualidade;

b) os registos de qualidade previstos na parte do sistema de qualidade dedicada à conceção, tais como resultados de análises, cálculos e ensaios;

c) os registos de qualidade previstos na parte do sistema de qualidade dedicada ao fabrico, tais como relatórios de inspeções, dados dos ensaios e de calibração e relatórios de qualificação do pessoal envolvido.

4.3. O organismo notificado deve efetuar auditorias periódicas para se certificar de que o fabricante mantém e aplica o sistema de qualidade e deve fornecer-lhe os relatórios dessas auditorias.

5. Marcação de conformidade e declaração de conformidade

5.1. O fabricante deve apor a marcação CE e, sob a responsabilidade do organismo notificado referido no ponto 3.1, o número de identificação deste último em cada produto com elementos digitais que cumpra os requisitos constantes da parte I do anexo I.

5.2. O fabricante deve elaborar uma declaração de conformidade escrita para cada modelo de produto e mantê-la à disposição das autoridades nacionais, por um período de 10 anos a contar da data de colocação do produto com elementos digitais no mercado ou durante o período de apoio, consoante o que for mais longo. A declaração de conformidade deve identificar o modelo de produto para o qual foi elaborada.

Deve ser disponibilizada às autoridades competentes, a pedido destas, uma cópia da declaração de conformidade.

6. O fabricante deve manter à disposição das autoridades nacionais, durante um período não inferior a 10 anos após a data de colocação do produto com elementos digitais no mercado ou durante o período de apoio, consoante o que for mais longo:

a) a documentação técnica referida no ponto 3.1;

b) a documentação relativa ao sistema de qualidade referida no ponto 3.1;

c) a alteração, aprovada, a que se refere o ponto 3.5;

d) as decisões e os relatórios do organismo notificado a que se referem os pontos 3.5 e 4.3.

7. Cada organismo notificado deve informar as suas autoridades notificadoras das aprovações de sistemas de qualidade concedidas ou retiradas e, periodicamente ou mediante pedido, deve disponibilizar a essas autoridades a lista das aprovações de sistemas de qualidade que tenha recusado, suspendido ou submetido a quaisquer outras restrições.

Cada organismo notificado deve informar os outros organismos notificados das aprovações de sistemas de qualidade que tenha recusado, suspendido, retirado e, se lhe for pedido, das aprovações que tenha concedido a sistemas de qualidade.

8. Mandatário

As obrigações do fabricante enunciadas nos pontos 3.1, 3.5, 5 e 6 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo respetivo mandatário, desde que as obrigações pertinentes se encontrem especificadas no mandato.

Foi feita uma declaração relativamente ao presente ato, que pode ser consultada em JO C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.